

## Consumer Compliance (CC)

# Compliance Management Systems

Version 1.0, June 2018

# Contents

---

<b>Introduction.....</b>	<b>1</b>
Compliance Management Systems Defined .....	1
Use of this Booklet.....	1
CMS Examinations .....	2
Community Reinvestment Act Considerations.....	3
Heightened Standards .....	3
Risks Associated With CMS.....	4
Compliance Risk.....	4
Operational Risk .....	4
Strategic Risk.....	5
Reputation Risk.....	5
<b>CMS Components .....</b>	<b>6</b>
Board and Management Oversight .....	6
Oversight and Commitment.....	6
Change Management .....	8
Comprehension, Identification, and Management of Risk .....	9
Self-Identification and Corrective Action.....	11
Consumer Compliance Program .....	11
Policies and Procedures .....	11
Consumer Compliance Training.....	12
Monitoring and Audit .....	13
Consumer Complaint Resolution Process.....	15
Violations of Law and Consumer Harm .....	16
<b>Examination Procedures .....</b>	<b>17</b>
Scope.....	17
Board and Management Oversight .....	18
Consumer Compliance Program .....	22
Conclusions.....	25
<b>Appendix.....</b>	<b>26</b>
Appendix A: Uniform Interagency Consumer Compliance Rating System (CC Rating System) .....	26
<b>References.....</b>	<b>37</b>

# Introduction

---

The Office of the Comptroller of the Currency’s (OCC) *Comptroller’s Handbook* booklet, “Compliance Management Systems,” is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and federal agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in this booklet consistent with each bank’s individual circumstances. When it is necessary to distinguish between them, national banks and federal savings associations are referred to separately.

The consumer compliance risk management principles in this booklet reflect the OCC’s risk-based supervision approach and are consistent with the OCC’s assessment of banks’ risk management systems and the interagency consumer compliance rating definition. The principles in this booklet do not set new or higher expectations for banks.

## Compliance Management Systems Defined

A bank’s overall compliance management system (CMS) includes policies, procedures, processes, monitoring and testing programs, and a compliance audit function regarding compliance with all applicable laws and regulations. The abbreviation “CMS” in this booklet refers to only those aspects of the bank’s overall CMS that pertain to the bank’s compliance with consumer protection-related laws and regulations. An effective CMS includes processes and practices designed to manage consumer compliance risk, support compliance with consumer protection-related laws and regulations, and prevent consumer harm. The primary components of a CMS that examiners consider when evaluating a bank’s CMS include board and management oversight and a compliance program. Table 1 outlines broadly what examiners consider when assessing board and management oversight and the compliance program, respectively.

**Table 1: CMS Components**

<b>Board and management oversight</b>	<b>Consumer compliance program</b>
<ul style="list-style-type: none"> <li>• Oversight and commitment, including oversight of third parties</li> <li>• Change management</li> <li>• Comprehension, identification, and management of risks</li> <li>• Self-identification and corrective action</li> </ul>	<ul style="list-style-type: none"> <li>• Policies and procedures</li> <li>• Consumer compliance training</li> <li>• Monitoring and audit</li> <li>• Consumer complaint response</li> </ul>

## Use of this Booklet

This booklet provides background information and examination procedures for assessing a bank’s CMS and assigning the consumer compliance component rating under the Uniform

Interagency Consumer Compliance Rating System (CC Rating System).<sup>1</sup> Examiners decide which examination procedures in this booklet to use, if any, during examination planning or after drawing preliminary conclusions during the compliance core assessment. Complaint information received by the Customer Assistance Group (CAG) in the OCC's Office of Enterprise Governance and the Ombudsman, by the Bureau of Consumer Financial Protection (BCFP),<sup>2</sup> and by the bank may also be useful in completing the core assessment or expanded procedures.

Aspects of a bank's overall CMS (i.e., those aspects not specific to consumer protection-related laws and regulations) should be considered when assessing the bank's overall risk management program and determining the management component rating. The assessment of compliance risk in the OCC's Risk Assessment System (RAS) considers the bank's compliance with all applicable laws and regulations (including those that extend beyond consumer protection-related laws and regulations). Refer to the "Bank Supervision Process," "Community Bank Supervision," "Federal Branches and Agencies Supervision," or "Large Bank Supervision" booklets of the *Comptroller's Handbook* for additional information regarding the core assessment, regulatory ratings, and the RAS.

## CMS Examinations

Examiners must review the bank's CMS during every supervisory cycle to complete the consumer compliance core assessment and assign the consumer compliance component rating. This may be done by conducting one supervisory activity or aggregating the results of multiple supervisory activities conducted during the supervisory cycle. The scope of the consumer compliance examination, including the review of CMS, should be risk-based, although there are some subject areas that must be reviewed each cycle, either because of a statutory requirement or because of an OCC policy decision. Unless otherwise required, examiners should use judgment in determining whether transaction testing is warranted when assessing the bank's CMS. Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for additional details on the scope of consumer compliance examinations.

When determining the consumer compliance component rating, examiners should consider the effectiveness of the bank's CMS for compliance with all applicable consumer protection-related laws and regulations (including, but not limited to, the Home Mortgage Disclosure Act [HMDA]<sup>3</sup> and fair lending-related laws and regulations [e.g., the Equal Credit

---

<sup>1</sup> The OCC, along with the other members of the Federal Financial Institutions Examination Council (FFIEC), issued the revised CC Rating System on November 7, 2016, to reflect current supervisory approaches for consumer compliance. Refer to 81 Fed. Reg. 79473, "Uniform Interagency Consumer Compliance Rating System," and to appendix A of this booklet.

<sup>2</sup> BCFP data are available for banks with total assets of more than \$10 billion. CAG data for banks with total assets of \$10 billion or less include complaints originally sent to the BCFP.

<sup>3</sup> Refer to "A Guide to HMDA Reporting: Getting It Right!" section 9.2, "Implementation and compliance management support activities," for information regarding HMDA-specific CMS considerations for banks.

Opportunity Act and the Fair Housing Act]). Examiners should also consider laws and regulations for which the BCFP is assigned exclusive supervisory authority under the Dodd–Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd–Frank).<sup>4</sup> Examiners must consider material information that the BCFP provides to the OCC when assigning the consumer compliance rating for banks with more than \$10 billion in total assets. OCC examiners generally may not, however, conduct transaction testing<sup>5</sup> or determine compliance with any law or regulation for which the BCFP is assigned exclusive supervisory authority under Dodd–Frank. Pursuant to the 2012 interagency memorandum of understanding on supervisory coordination,<sup>6</sup> the OCC has established protocols for communicating material supervisory information to the BCFP. When OCC examiners identify a bank’s potential non-compliance with any law or regulation where the BCFP is assigned supervisory authority, examiners should consult with their supervisory office and follow OCC-established processes.

## Community Reinvestment Act Considerations

The CC Rating System does not consider a bank’s CRA performance, as CRA performance is evaluated separately and assigned its own component rating. Examiners should consult with appropriate Compliance Supervision Management, Compliance Risk Policy, or Legal representatives when considering CRA programmatic or risk management deficiencies in the CMS review.

## Heightened Standards

12 CFR 30, appendix D, “OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches,”<sup>7</sup> applies to banks with average total consolidated assets of \$50 billion or greater or those that the OCC designates as covered banks. For covered banks, certain CMS components discussed in this booklet may also need to be incorporated into the heightened

---

<sup>4</sup> Section 1025 of Dodd–Frank (12 USC 5515) granted the BCFP exclusive authority to examine insured depository institutions with more than \$10 billion in total assets and their affiliates for compliance with enumerated Federal consumer financial laws. Refer to 12 USC 5481 for the definition of enumerated Federal consumer financial laws. The prudential regulators retained authority for examining insured depository institutions with more than \$10 billion in total assets for compliance with certain other laws related to consumer financial protection, including the Fair Housing Act, Servicemembers Civil Relief Act (SCRA), and section 5 of the Federal Trade Commission Act.

<sup>5</sup> Examiners may conduct transaction testing in banks with assets of more than \$10 billion to verify the accuracy and reliability of data a bank reports under the HMDA and Regulation C for use in CRA or fair lending examinations. Examiners may not cite violations in such cases but may direct the bank to correct the data before use in CRA or fair lending examinations.

<sup>6</sup> Refer to OCC News Release 2012-85, “Memorandum of Understanding on Supervisory Coordination.”

<sup>7</sup> Refer to 12 CFR 30, appendix D, I.E.5, and to OCC Bulletin 2014-45, “Heightened Standards for Large Banks; Integration of 12 CFR 30 and 12 CFR 170: Final Rules and Guidelines.”

standards identified in 12 CFR 30, appendix D. Refer to the “Corporate and Risk Governance” booklet of the *Comptroller’s Handbook* for additional information regarding heightened standards.

## Risks Associated With CMS

From a supervisory perspective, risk is the potential that events will have an adverse effect on a bank’s current or projected financial condition<sup>8</sup> and resilience.<sup>9</sup> The OCC has defined eight categories of risk for bank supervision purposes: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. These categories are not mutually exclusive. Any product or service may expose the bank to multiple risks. Risks also may be interdependent and positively or negatively correlated. Examiners should be aware of and assess the effect of this interdependence. Refer to the “Bank Supervision Process” booklet of the *Comptroller’s Handbook* for additional discussion of banking risks and their definitions. The primary risks associated with a bank’s CMS are compliance, operational, strategic, and reputation. These risks are discussed in more detail in the following paragraphs.

### Compliance Risk

Compliance risk is the risk to a bank’s current or projected financial condition and resilience arising from violations of laws or regulations or from nonconformance with prescribed practices, internal bank policies and procedures, or ethical standards. The OCC expects the board and management, collectively, to be responsible for the bank’s compliance with all applicable laws and regulations. Failure to establish a sound CMS, which addresses all applicable consumer protection-related laws and regulations, exposes the bank to increased legal and reputation risks and the potential for enforcement actions (including civil money penalties [CMP]), and customer reimbursements. Compliance risk can result in diminished reputation, harm to bank customers, limited business opportunities, and lessened expansion potential.

### Operational Risk

Operational risk is the risk to current or projected financial condition and resilience arising from inadequate or failed internal processes or systems, inappropriate accounting, human errors or misconduct, or adverse external events. Operational risk may be elevated when banks have higher volumes of loans, larger numbers of transactions processed, and more extensive use of automation and technology. Highly automated environments pose heightened operational risk exposure that can result in compliance or reputation risk, as automated environments can compound the exposure of errors. Operational risk can also

---

<sup>8</sup> Financial condition includes effects from diminished capital and liquidity. Capital in this context includes potential effects from losses, reduced earnings, and market value equity.

<sup>9</sup> Resilience recognizes the bank’s ability to withstand periods of stress.

result when a bank outsources operational functions (e.g., loan origination, account management, collections, payment processing, data input, and legal assistance) to third parties.<sup>10</sup>

## Strategic Risk

Strategic risk is the risk to current or projected financial condition and resilience arising from adverse business decisions, poor implementation of business decisions, or lack of responsiveness to changes in the banking industry and operating environment. Additionally, strategic risk increases when new activities are not compatible with the bank's risk appetite or strategic plan or do not provide an adequate return on investment; the bank engages in new activities without performing adequate due diligence, including upfront expense analysis; or management does not have adequate resources, expertise, and experience to properly implement and oversee the new activities. New activities should be developed and implemented consistently with sound risk management practices and should align with banks' overall business plans and strategies. New activities should encourage fair access to financial services and fair treatment of consumers and should be in compliance with applicable laws and regulations.<sup>11</sup> The board and senior management, collectively, are the key decision makers who drive the strategic direction of the bank and establish governance principles. The failure to integrate the bank's CMS into its decision-making and implementation process can have wide-ranging consequences. The consequences may include missed business opportunities, losses, failure to comply with laws or regulations, or deficient practices (including those that are unsafe or unsound) that could lead to enforcement actions, including CMPs.

## Reputation Risk

Reputation risk is the risk to earnings, capital, or enterprise value arising from negative public opinion. This risk may impair the bank's competitiveness by affecting its ability to establish new relationships or services or continue servicing existing relationships. Inadequate policies and procedures, operational breakdowns, or other weaknesses in the bank's CMS can harm its reputation when these weaknesses result in violations of consumer protection-related laws or regulations, particularly when consumers are harmed. Inappropriate delegation of activities to third parties and wrongful acts by third parties acting on the bank's behalf may also increase a bank's reputation risk exposure. Effective systems and controls to identify, measure, monitor, and control potential issues, such as appropriate oversight of sales, servicing, and collection practices, are important to managing risks, including reputation, compliance, and operational risks.

---

<sup>10</sup> Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," and OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures," for more information regarding third-party risk management.

<sup>11</sup> Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles."

# CMS Components

---

CMS is the method by which a bank manages consumer compliance risk, supports compliance with consumer protection-related laws and regulations, and prevents consumer harm. The complexity of the compliance risk environment presents challenges for banks. The volume and complexity of consumer protection-related laws and regulations coupled with changing technologies and earnings pressures increase the importance of a bank's CMS. Each bank should develop and maintain an effective CMS that is appropriate for the size, complexity, and risk profile of its operations. The CMS should consist of board and management oversight and a compliance program that includes all applicable consumer compliance-related laws and regulations.

The consumer compliance rating takes into account the effectiveness of the bank's CMS and factors relating to violations of law and consumer harm. Refer to the "Violations of Law and Consumer Harm" section and appendix A of this booklet for additional information.

## Board and Management Oversight

Board and management oversight should be commensurate with the bank's size, complexity, and risk profile. Oversight should factor in all applicable consumer protection-related laws and regulations and include consumer compliance expectations for third-party relationships. It is important for the board and management to understand the potential consequences of violations of laws and regulations that may result in customer reimbursements, financial losses, reputation risks, and legal risks, including enforcement actions (including CMPs). In relation to their respective roles, board and management oversight should include the following:

- Oversight of and a commitment to the bank's CMS, including oversight of third parties.
- Effective change management processes, which include responding in a timely and satisfactory manner to any change, internal or external, to the bank.
- Comprehension, identification, and management of risks arising from the bank's products, services, or activities.
- Self-identification of consumer compliance issues and timely correction of such issues.

## Oversight and Commitment

The board and management should demonstrate a commitment to and oversight of the bank's CMS.<sup>12</sup> The board should oversee, and management should implement, a consumer compliance program with effective resources, including

---

<sup>12</sup> Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for additional information regarding the roles of the board and management in establishing an appropriate compliance culture that incorporates all applicable laws and regulations, including consumer protection-related laws and regulations.

- systems, capital, and human resources commensurate with the bank’s size, complexity, and risk profile.
- knowledgeable staff who are appropriately trained, empowered, and held accountable for compliance with consumer protection-related laws and regulations.

## **Board of Directors**

The board should create a culture that places a priority on compliance and holds management accountable. The board plays a pivotal role in the effective governance of the bank, including oversight of the bank’s CMS. The board should oversee management, provide organizational leadership, and establish core corporate values. The board should oversee management’s implementation of the bank’s CMS and hold management accountable for implementing a CMS that is consistent with the bank’s strategic direction, risk culture, and risk appetite.

The board should receive sufficient consumer compliance-related information including management information systems (MIS) reports, risk assessments, and monitoring and independent audit reports to assess the effectiveness of the bank’s CMS and, when appropriate, provide credible challenge to management. Applicable board or board committee minutes should reflect the board’s or committee’s receipt and deliberation of information related to the bank’s consumer compliance risk management practices and the effectiveness of those practices to manage consumer compliance risk, support compliance with consumer protection-related laws and regulations, and prevent consumer harm. The board should understand its roles and responsibilities related to consumer compliance, and periodically assess directors’ consumer compliance skills and competencies relative to the bank’s size, complexity, and risk profile. Management can support the board by instituting an ongoing education and training program that includes consumer compliance to keep the board informed and current on general industry trends and regulatory developments, particularly regarding issues that pertain to the bank.

## **Bank Management**

The board generally delegates authority to management for directing and overseeing day-to-day operations of the bank, including developing and implementing the bank’s CMS consistent with the board’s strategic objectives and risk appetite. Management should monitor the performance of the compliance program, including

- third-party risk management processes that include due diligence and ongoing monitoring of third parties (i.e., third-party risk management processes).
- change management.
- comprehension, identification, and management of risk.
- self-identification of compliance risk management deficiencies and corrective action.

Management may use committees to facilitate oversight of day-to-day banking activities, including consumer compliance-related activities. Management should determine which committees are appropriate for the bank and how formal each committee’s structure should

be. Examples of consumer compliance-related committees may include compliance risk management and fair banking.

Management also should establish and clearly communicate compliance-related roles and responsibilities. Regardless of the form of the compliance function, management should provide it with appropriate resources, including systems, capital, and human resources. Many banks establish a separate compliance function headed by a compliance officer. In such banks, the compliance officer should have the authority and independence to facilitate compliance throughout the bank and sufficient time and resources, including staff, to execute assigned duties. The compliance officer should have the appropriate skills and knowledge of the consumer protection-related laws and regulations applicable to the bank. Compliance officers should oversee the compliance training for all bank employees. For banks with limited staff or overlapping compliance and other responsibilities, training and development is particularly important to conduct continuous and consistent operations. Additionally, the compliance officer should be afforded opportunities for external training to maintain or refresh his or her subject matter expertise pertinent to overseeing the bank's compliance program.

### **Third-Party Risk Management**

There can be certain benefits to banks engaging in relationships with third parties, including gaining operational efficiencies or an ability to deliver additional products and services. Third-party relationships may expose the bank to risks, if not managed effectively. While management may make the business decision to outsource some or all of the operational aspects of a product or service, the bank cannot outsource the responsibility for complying with consumer protection-related laws and regulations or managing the consumer compliance risks associated with products or services offered by the third party. Management should implement third-party risk management processes commensurate with the level of risk and complexity presented by the third-party relationships. The bank's third-party risk management process should include the following specific to consumer compliance:

- Due diligence and ongoing monitoring of third parties to assess compliance with consumer protection-related laws and regulations.
- Oversight of third parties' consumer compliance-related policies, procedures, internal controls, and training.

Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," and OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures," for additional information regarding third-party risk management.

### **Change Management**

Specific to consumer compliance, management should anticipate and respond in a timely manner to changes in applicable consumer protection-related laws and regulations, market

conditions, and products and services offered by evaluating the change and implementing responses across affected lines of business. Management should have a process to identify laws and regulations applicable to the bank's activities and stay abreast of evolving regulatory requirements. The formality of the change management process should be commensurate with the bank's size, complexity, and risk profile.

Management should conduct due diligence in advance of engaging in new, modified, or expanded products or services, consider the entire lifecycle of a product or service in implementing change, and review the change after implementation to determine that actions taken have achieved planned results. The compliance function should be involved in the due diligence and monitoring of new, modified, or expanded products or services. Refer to OCC Bulletin 2017-43, "New, Modified, or Expanded Bank Products and Services: Risk Management Principles," for additional information.

## Comprehension, Identification, and Management of Risk

Management should comprehend, identify, and manage consumer compliance risks, including existing and emerging risks to the bank's products, services, and other activities.

The sophistication of risk management should be proportionate to the risks present and the bank's size and complexity. Regardless of the bank's size and complexity, sound management of consumer compliance risk should do the following:

**Identify risk:** The board and management should identify existing risks and risks that may arise from new business initiatives, including risks that originate in nonbank subsidiaries, affiliates, and third-party relationships and those that arise from external market forces or regulatory or statutory changes. Risk identification should be a continual process and should occur at the transaction, portfolio, and enterprise levels. For larger, more complex banks, the board and management also should identify interdependencies and correlations across portfolios and lines of business that may amplify risk exposures. Proper risk identification is important for banks to determine that risks are addressed appropriately.

**Measure risk:** Accurate and timely measurement of risks is important to effective risk management systems. A bank that does not have a risk measurement system has limited ability to control or monitor risk levels. Further, the bank should have more sophisticated measurement tools as the complexity of the risk increases. Management should periodically conduct tests to verify that the bank's measurement tools are accurate. Sound risk measurement systems assess the risks at the individual transaction, portfolio, and enterprise levels. Larger, more complex companies should pay particular attention to assessing the effect of increased transaction volumes across all risk categories.

**Monitor risk:** Management should monitor risk levels to confirm timely review of risk positions and exceptions, including throughout business combination and reorganization activities. Management-developed and -implemented monitoring reports should be timely and accurate and should be distributed to appropriate individuals, including the board, to initiate action, when appropriate. For larger, more complex banks, monitoring is important to

confirm that management's decisions are implemented for all geographies, products and services, and legal entities. Well-designed monitoring systems allow the board to hold management accountable for operating within established risk appetites.

**Control risk:** The board should determine that risk limits are communicated through policies, standards, and procedures that define responsibility and authority. These limits should serve as a means to control exposures to the various risks associated with the bank's activities. The limits should be tools that, based on board approval, can be adjusted when conditions or risk appetites change. Management should have a process to document adherence to established limits, and to authorize, document, and report to the board exceptions to risk limits. Large, diversified banks should have strong risk controls covering all geographies, products and services, and legal entities to prevent undue exposure from concentrations of risk.

## Risk Assessment

The bank's CMS should include a consumer compliance risk assessment process commensurate with the size, complexity, and risk profile of the bank. Completing risk assessments helps management identify current and emerging consumer compliance risks in order to prevent, self-identify, and address potential consumer compliance issues. A well-designed risk assessment process should be supported by appropriate methodology that includes quantitative and qualitative data and evaluates risk across all products, services, and lines of business. An effective risk assessment process helps the board and management address emerging risks at an early stage and allows them to proactively develop and implement appropriate strategies to mitigate the risks before the risks have an adverse effect on the bank's condition or risk profile.

Management should perform or update the bank's consumer compliance risk assessment periodically, based on the bank's size, complexity, and risk profile. The sophistication of the risk assessment process should be commensurate with the bank's size, complexity, and risk profile. In less complex banks, it may be appropriate to have a single compliance risk assessment evaluating all products, services, and business lines. In more complex banks, the risk assessment process may involve completing multiple compliance risk assessments, with results of individual risk assessments aggregated into an overall compliance risk assessment that considers and evaluates consumer compliance risk at the enterprise level. While an effective risk assessment process may look different across banks, each risk assessment should evaluate and make determinations regarding the following:<sup>13</sup>

- Inherent risk, which is the risk that an activity would pose if no controls or mitigating factors were in place.
- Residual risk, which is the level of risk after controls are taken into account.

---

<sup>13</sup> Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for more information regarding risk assessments.

## Self-Identification and Corrective Action

Management should identify, respond to, and remediate violations of laws or regulations and deficient practices in a timely manner. Moreover, self-identification and prompt correction of violations and deficient practices may reflect strengths in the bank's CMS and could indicate management's and the board's commitment to address responsibly underlying consumer compliance risk. Appropriate corrective action should remedy harmed parties, correct programmatic weaknesses related to the violation, and prevent violations from occurring in the future.

### Issues Management

Issues management refers to processes for tracking, escalating, and resolving issues (e.g., deficient practices, violations, or other weaknesses) identified across the bank. Traditionally, internal audit has been responsible for maintaining formal processes to track and follow up on issues identified through audits and regulatory examinations. Issues can also surface from other sources, however, including quality control and quality assurance processes, monitoring and testing by the compliance function, control gaps identified through the risk assessment process, management's self-identification of issues, and adverse trends identified from monitoring of consumer complaints. Management should design and implement an issues management process that incorporates all sources of risk and issue identification. The issues management process should include identification of root causes of issues and determining whether issues are related to a specific product, service, or business line or if issues are systemic. The board should be apprised of material issues and resolution strategies, and hold management accountable for correcting issues and validating corrective actions.

## Consumer Compliance Program

An effective consumer compliance program should include the following:

- Policies and procedures that are appropriate to the complexity and risk in the bank's products, services, and activities, including an appropriate third-party risk management process.
- Consumer compliance training that is current and tailored to risk and staff responsibilities.
- Monitoring and, if applicable, audit that encompass consumer compliance risks throughout the bank.
- A responsive and effective consumer complaint resolution process.

### Policies and Procedures

Consumer compliance policies and procedures, including those for the bank's third-party risk management process, should provide standards for managing consumer compliance risk in the bank's products, services, and activities.

Policies are statements of actions that the bank adopts to pursue certain objectives. Policies guide decisions and often set standards (on risk limits, for example) and should be consistent with the bank's underlying mission, strategy, risk appetite, and core values.

The scope and detail of those policies should vary depending on the bank's size, complexity, and risk profile. A smaller, noncomplex bank with management that is heavily involved in the bank's day-to-day operations should have basic policies addressing the significant areas of consumer compliance risk. Larger, more complex banks, where senior management relies on a widely dispersed staff to manage consumer compliance risks associated with complex or varied products, services, and activities, should have more detailed policies. Appropriate policies should be in place and approved by the board before the bank engages in any new or significantly changed consumer compliance-related activities.

Procedures define how the bank is to carry out its policies. Management should consider the complexity and risk associated with products, services, and activities when determining the level of formality needed for consumer compliance-related procedures. Procedures should be consistent with related bank policies.

## Consumer Compliance Training

Consumer compliance training should be timely, and specifically tailored to employees' job functions and the bank's products, services, and level of risks. Training should span the entire organization, including staff responsible for product development, marketing, and customer service. Banks should train business line employees on consumer compliance requirements and bank procedures. The compliance and audit functions should have access to more advanced or specialized training, including emerging risks, trends, and industry developments, and training on compliance-related policies and procedures. Training for the board and management is generally focused on their individual responsibilities to oversee and govern the bank's CMS.

Standards for the frequency, method (e.g., formal, on-the-job, external), and documentation of training should be addressed in policies and procedures. For example, some laws impose mandatory training requirements. Periodic training increases the likelihood of adherence to the bank's policies and procedures and to changing legal requirements. Records, including training content, attendees, and completion dates, should be maintained to demonstrate the effectiveness of the bank's training program. The method and documentation of training may vary depending on the size of the bank or department, established time frames for training, and the significance and complexity of the subject matter.

The consumer compliance training program should be updated in advance of the introduction of new products, services, activities, or the effective date of new consumer protection-related laws and regulations to ensure that all staff are aware of compliance requirements before such changes occur.

## Monitoring and Audit

Monitoring of consumer compliance risk is a key aspect of an effective CMS that involves both the evaluation and reporting of risks. Consumer compliance risk identification and assessment activities, such as risk control self-assessments, quality assurance, and quality controls, are integral to monitoring by providing ongoing or periodic evaluation of the bank's consumer compliance risk environment. To facilitate monitoring of consumer compliance risk, the bank's CMS should include bank-wide monitoring inclusive of the bank's products, services, and activities.

Management's assessment of consumer compliance risk associated with the bank's products, services, activities, and processes may assist the bank in determining the extent, depth, frequency, and focal points of independent consumer compliance audits. For instance, monitoring may be appropriate for products, services, activities, or processes that are less complex or demonstrate less risk. The board may require an independent consumer compliance audit to determine the bank's compliance with consumer protection-related laws and regulations, particularly for more complex, higher-risk products, services, activities, or processes. Additionally, a periodic and independent audit of the bank's CMS should provide the board with information to determine the effectiveness of the bank's CMS.

Monitoring and audit activities should be timely and should identify and measure material consumer compliance risk throughout the bank. Monitoring and audit of the bank's compliance program should be proactive in identifying procedural or training weaknesses to preclude consumer protection-related violations. Compliance program modifications made to address identified weaknesses should be implemented expeditiously to minimize consumer compliance risk.

### Monitoring

Effective monitoring and testing include quality control and quality assurance<sup>14</sup> and identify violations of consumer protection-related laws or regulations or non-compliance with bank policies and procedures. Effective monitoring also provides timely identification of CMS deficiencies or weaknesses and can limit the size and scope of consumer harm by providing for timely corrective action.

Monitoring is generally more frequent and less formal than the independent review performed by the audit function. The plan and schedule for monitoring activities, however, should be risk-based, documented, and updated at least annually. Management, in consultation with the board, should determine the frequency, scope, and formality of monitoring and testing. Depending on the size, complexity, and risk of the bank, staff responsible for monitoring and testing may have less independence than the audit function's staff. Management should clearly outline roles and responsibilities so that monitoring by the various groups is complementary and not duplicative.

---

<sup>14</sup> Refer to the "Corporate and Risk Governance" booklet of the *Comptroller's Handbook* for additional information regarding quality control and quality assurance.

Transaction testing is an important component of monitoring. A bank's sampling methodology should incorporate appropriate sampling techniques. Transaction testing may be conducted by compliance staff or within business lines. Other forms of monitoring may include employee interviews, policy and procedure review, assessing training effectiveness, and comparison of actual practices with disclosures provided in connection with transactions.

The bank should complete root cause analyses to determine whether identified violations of law or regulation or failures to follow established policies and procedures are isolated events or systemic. Identified issues should be escalated and tracked in accordance with the bank's issues management policies and procedures. Additionally, the root cause determination should identify whether existing controls should be enhanced or if new controls should be implemented.

## **Audit**

The bank's internal audit system<sup>15</sup> should include risk-based independent reviews of the bank's CMS to provide the board and management reasonable assurance of the bank's consumer compliance-related risk management. Inclusion of CMS in the audit program substantially lessens the risk of a bank failing to detect potentially serious problems, such as non-compliance with consumer protection-related laws or regulations. The bank's risk-based internal audit coverage over CMS should include the following:

- Independent and qualified auditors who are knowledgeable of consumer protection-related laws and regulations and can assess the appropriateness of the bank's CMS.
- Testing of internal controls to identify
  - inaccurate, incomplete, or unauthorized transactions.
  - violations of consumer protection-related laws or regulations.
  - deviations from the bank's consumer compliance-related policies and procedures.
  - thematic consumer compliance control issues, including the root cause, across business activities or auditable entities.
- Evaluating the adequacy of established consumer compliance-related policies and procedures and identifying non-compliance with the bank's consumer compliance risk management processes.
- Reviewing and validating management actions to address material consumer compliance-related weaknesses.

The bank's audit risk assessment process should include identification of consumer compliance-related auditable entities, including third parties. The bank may perform a separate audit to evaluate the overall effectiveness of the bank's CMS, while audit coverage for consumer protection-related laws and regulations may encompass several individual audits or continuous auditing activities.

---

<sup>15</sup> Refer to 12 CFR 30, appendix A, II.A, "Operational and Managerial Standards," and the "Internal and External Audits" booklet of the *Comptroller's Handbook* for information regarding internal audit systems, including compliance audit systems.

The bank's process to track, monitor, report, and follow up on audit issues should include consumer compliance-related audit issues.

## Consumer Complaint Resolution Process

Consumer complaints can be an indicator of potential risk management weaknesses or other deficiencies, such as violations of laws or regulations. Complaints can reveal a weakness in a particular bank product, service, function, or department, or can identify opportunities to enhance customers' experience and understanding of bank products or services. Complaints can help banks assess services performed by third parties. While the absence of complaints is not conclusive of a strong CMS, the presence of complaints, especially multiple complaints regarding the same or similar issue, may indicate a weakness in the bank's CMS.

Banks should have a process for identifying, managing, and analyzing complaints. The formality of the process should be commensurate with the bank's size, complexity, and risk profile. An effective complaint resolution process should generally include the following:

- How the bank defines a complaint and requirements for documentation of complaints. With changing technology, complaints can come in many forms or through various channels: letters, phone calls, in person, other regulators, third-party service providers, emails, and even social media. Bank policies and procedures should address how these various types of complaints are documented and tracked.
- Responsibility and accountability for identifying, addressing, and escalating complaints.
- Tracking of complaints and bank responses or actions. A centralized tracking process can improve the identification of trends or patterns.
- Analysis of complaints to determine if a trend or pattern exists, and identifying the root cause of significant trends.
- Reporting complaint data and trends to the board and management.

Procedures should identify who is responsible for addressing complaints and detail the escalation process, including an alternative process for complaints involving the employee(s) tasked in the standard escalation process. Analysis of complaint data should be reported to the board and management to

- identify areas of concern relating to compliance management and consumer protection; and
- enable the bank to take proactive steps to mitigate risk of violations, consumer harm, regulatory actions, and legal action.

## Violations of Law and Consumer Harm

A violation of law or regulation is an act (or failure to act) that deviates from, or fails to comply with, a statutory or regulatory requirement. Violations (or lack of violations) alone are not conclusive to determine the effectiveness of a bank's CMS. Examiners should consider the nature, extent, severity, and root cause of violations when assessing the bank's CMS. Also, a bank's CMS can be weak when no violations are identified, if one or more components are absent or ineffective.

Violations often result from deficient practices. The existence of violations can be indicative of weaknesses in the bank's CMS. Violations that result from deficiencies in component(s) of the bank's CMS may be indicative of weak or lax board oversight or lack of management involvement in day-to-day operations of the CMS.

The bank's CMS should include processes for timely self-identification and appropriate resolution of violations. Timely self-identification and correction may support a conclusion that monitoring and compliance audit activities are being carried out effectively.

Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook* for additional information regarding the OCC's policies and procedures regarding violations of laws and regulations.

# Examination Procedures

---

This booklet contains objectives and expanded procedures for assessing the effectiveness of a bank's CMS in relation to consumer compliance risk management. Examiners decide which of these objectives and procedures are relevant to the scope of the examination during examination planning or after drawing conclusions during the compliance core assessment as outlined in the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook*.

## Scope

These procedures are designed to help examiners tailor the examination to each bank and determine the scope of the CMS examination. This determination should consider work performed by internal and external auditors and other independent risk control functions and by other examiners on related areas. Examiners need to perform only those objectives and examination procedures that are relevant to the scope of the examination as determined by the following objective.

**Objective:** To determine the scope of the CMS examination and identify examination objectives and activities necessary to meet the needs of the supervisory strategy for the bank.

1. Review, as applicable, the following sources of information and reports, and note any previously identified consumer compliance deficiencies related to CMS that require follow-up:
  - Supervisory strategy.
  - Examination scope memorandum.
  - The OCC's supervisory information system.
  - Previous reports of examination, supervisory letters, and work papers.
  - Consumer compliance-related supervisory information obtained from other regulatory agencies.
  - Internal and external audit reports and work papers.
  - Bank management's responses to previous reports of examinations, supervisory letters, and audit reports.
  - Customer complaint and litigation data, including data from the OCC CAG, the BCFP, and the bank. Coordinate with the examiner responsible for completing the compliance RAS and core assessment to avoid duplicating complaint data review.
  - Whistleblower referrals received by the OCC or internally within the bank. Coordinate with the examiner-in-charge (EIC), as the EIC may already possess this information.
2. Obtain and review consumer compliance-related policies, procedures, and reports the board and bank management use to evaluate the effectiveness of the bank's CMS. Examiners should consider

- board meeting packages, including committee reports and meeting minutes.
  - board compliance training materials.
  - the strategic plan and reports used to monitor the plan.
  - operational plans.
  - a list of new products, services, and systems and documentation of the due diligence and approval process.
  - third-party relationship risk management process, including policies and procedures.
  - executive and frontline unit MIS reports.
  - internal consumer compliance risk assessments.
  - consumer compliance policies and procedures, including the compliance management program.
  - compliance monitoring (including quality control and quality assurance), testing, and audit plans, schedules, and reports.
  - bank reports related to consumer compliance issues management, complaints, and litigation activity.
3. In discussions with management, determine if any significant consumer compliance-related changes (e.g., in policies, procedures, personnel, control systems, third-party relationships, products, services, delivery channels, volumes, markets, and geographies) have occurred since the prior examination of CMS.

## **Board and Management Oversight**

**Objective:** To determine whether the board and management provide sufficient oversight and create a culture that places a priority on consumer compliance. To determine whether the board is provided sufficient information to assess the effectiveness of the bank's CMS and, when appropriate, provide a credible challenge to management.

1. Hold discussions with management and review board minutes and other communications to the board and management. Determine whether
  - the board creates a culture that places a priority on consumer compliance, and that management further supports the culture through communications with staff.
  - consumer compliance-related board meeting agenda items receive appropriate review and deliberation by the board.
  - CMS policies and procedures include focus on consumer compliance, are reviewed by management regularly, and are approved by the board, as appropriate.
  - information—including consumer compliance-related MIS reports, risk assessments, and monitoring and independent audit reports that are provided to the board and management—is accurate, complete, timely, and presented in a meaningful format to allow for effective oversight.
  - the board periodically reevaluates information it receives to determine if it has sufficient information to make informed decisions, including decisions regarding the effectiveness of the bank's CMS, and to provide credible challenge to management's decisions and recommendations.

**Objective:** To determine whether management has hired, developed, and oversees a qualified compliance staff, including a compliance officer, capable of ensuring all of the bank's products, services, and operations comply with all applicable laws and regulations.

1. Through review of job descriptions, organizational charts, staff resumes, and discussions with management, determine whether
  - there is appropriate compliance staffing in relation to the bank's size, complexity, and risk profile.
  - the compliance officer and staff have appropriate skills and knowledge to manage the broad range of laws and regulations applicable to the bank and the compliance officer's and staff's duties.
  - the board and management provide the compliance officer with sufficient time and resources, including staffing, to implement and maintain the bank's CMS, commensurate with the bank's size, complexity, and risk profile.
  - the board and management provide the compliance officer with sufficient authority to carry out the responsibilities of that position, so that compliance with all laws and regulations is an organizational priority.
  - the compliance officer is organizationally separated and has sufficient independence from business units.
  - management has developed appropriate metrics to monitor the compliance officer's and compliance-related staff's performance and provide periodic updates to the board.

**Objective:** To determine whether management has implemented a third-party risk management process that is commensurate with the level of risk and complexity presented by the bank's third-party relationships.

1. Through review of applicable policies and procedures and discussions with management, determine whether the third-party risk management process includes, as appropriate
  - comprehensive initial and ongoing due diligence, and ongoing monitoring, of third-party relationships to assess compliance with consumer protection-related laws and regulations.
  - oversight of third parties' consumer compliance-related policies, procedures, internal controls, and training.
2. Review a sample of the bank's third-party due diligence and ongoing monitoring reports to determine whether the bank's process is appropriate and functioning as intended.

**Objective:** To determine whether management has implemented risk management processes over the bank's technology and automated systems used in consumer compliance management processes.

1. Through review of a list of consumer compliance-related systems and applications, and through discussions with management, determine whether management

- applies appropriate general technology controls related to confidentiality, integrity, and availability of the systems and data.
- completes sufficient testing and monitoring of automated processes to be able to rely on the accuracy of the outcomes, calculations, and disclosures generated.
- includes systems and applications in its change management processes to re-test results when regulatory changes occur or when changes are made to the systems.
- includes these systems and applications in the scopes of reviews and audits, as appropriate, and commensurate with the risk.

**Objective:** To determine whether the bank has a change management process that is commensurate with its size, complexity, and risk profile.

1. Through review of applicable policies and procedures and discussions with management, determine whether
  - management monitors market conditions and regulatory developments to identify and communicate to staff upcoming changes in applicable consumer protection-related laws and regulations, market conditions, and services offered, and takes appropriate steps in advance of changes to prepare the bank to respond to changes once they occur.
  - upcoming changes are communicated to customers as needed, including timely issuance of any required disclosures or account agreements.
  - changes are evaluated and responses are implemented across all affected lines of business.
  - management conducts due diligence in advance of product changes, considers the entire life cycle of a product or service in implementing change, and reviews the change after implementation to determine that actions taken achieved planned results.
2. Review the bank's completed consumer compliance-related change management activities to determine whether the bank's process is appropriate and functioning as intended. Information to review may include the bank's project management tracking records, applicable committee meeting minutes, adopted policies and procedures related to the change, and monitoring or audit reports for reviews conducted throughout and after the change.

**Objective:** To determine whether management has instituted an effective consumer compliance risk management process that

- is commensurate with the size, complexity, and risk profile of the bank.
- effectively demonstrates management's understanding of and ability to identify consumer compliance risks, including emerging risks to the bank's products, services, and other activities.
- demonstrates management is actively engaged in managing consumer compliance risks, including through self-assessments (i.e., consumer compliance risk assessments).

1. Through review of the bank's consumer compliance risk assessment(s), related policies, procedures, methodology, and discussions with management, determine whether the bank's consumer compliance risk assessment is
  - developed and implemented by management, periodically reviewed, and approved by the board.
  - commensurate with the bank's size, complexity, and risk profile in its formality and sophistication.
  - inclusive of qualitative conclusions that are supported by quantitative data regarding the quantity of risk, quality of risk management, aggregate risk, and the direction of risk. (Banks may use similar terminology in relation to quantity of risk, quality of risk management, aggregate risk, and direction of risk, such as inherent risk, effectiveness of controls, residual risk, and key risk indicators.)
  - performed or updated periodically based on risk events and the size, complexity, and risk profile of the bank.
  - periodically reviewed and validated by internal audit for reasonableness and accuracy.
  
2. Through review of MIS reporting and discussions with management, determine whether
  - the bank has an appropriate process to continuously monitor consumer compliance risk and to promptly report, including to the board, risk positions and risk exceptions.
  - consumer compliance risk monitoring includes all of the bank's geographies, products and services, business units, and legal entities.
  - consumer compliance risk monitoring systems provide the board with timely and sufficient information to determine whether management operates within the bank's established risk appetite, and to take action, as appropriate.

**Objective:** To determine whether management implements appropriate self-identification and corrective action into the bank's CMS.

1. Determine whether management self-identifies issues and promptly corrects consumer compliance risk management deficiencies and violations of laws or regulations by remediating consumer harm when necessary.
2. Determine whether consumer protection-related laws and regulations are included in the bank's CMS to assist in preventing consumer compliance violations or to facilitate early detection of potential violations and to limit the size and scope of consumer harm.
3. Through a review of the bank's processes for tracking, escalating, resolving, and reporting consumer compliance issues, determine whether the bank is capturing identified issues across all business units and through all channels, including

- internal audit and regulatory examinations.
- quality control and quality assurance processes.
- compliance monitoring and testing.
- compliance risk assessment process.
- complaints.

## Consumer Compliance Program

**Objective:** To determine whether management has developed and implemented appropriate consumer compliance-related policies and procedures that are comprehensive and provide standards to effectively manage consumer compliance risk in the bank's products, services, and activities.

1. Through review of applicable consumer compliance policies and procedures and through discussions with management, determine whether
  - policies address significant consumer compliance activities and risk and are commensurate with the bank's size, complexity, and risk profile.
  - management develops and institutes appropriate policies before engaging in new consumer compliance-related activities.
  - management appropriately determines whether to develop, and level of formality for, consumer compliance-related procedures, and whether the procedures address how the bank is to carry out consumer compliance-related policies.

**Objective:** To determine the appropriateness of consumer compliance training.

1. Through review of training materials, completion records, and discussions with management, determine whether
  - the board and management place a priority on consumer compliance training and incorporate training requirements into job performance evaluations.
  - training is ongoing and tailored to job function and responsibilities, with higher-risk functions (e.g., compliance staff and internal audit) having access to specialized or advanced training that includes emerging risks, trends, and industry developments.
  - management monitors training results to confirm staff is completing training within established time frames, and periodically reports results to the board.
  - management proactively provides consumer compliance training in advance of the introduction of new products, services, or activities, or new consumer protection-related laws and regulations, to confirm that all staff are aware of compliance requirements before changes occur.
  - the board and management receive appropriate training, including training that focuses on their individual responsibilities to oversee and govern the bank's CMS.

**Objective:** To determine the effectiveness of the bank's compliance monitoring and testing.

1. Assess the effectiveness of the compliance monitoring and testing function. Evaluate
  - the frequency and scope.
  - the transaction sampling methodology.
  - the qualifications of staff responsible for monitoring and testing.
  - the adequacy of reporting findings to the board and management.
  - whether findings include a root cause determination and are corrected in a timely and appropriate manner.

**Objective:** To determine, as applicable, the adequacy of the bank’s compliance audit function, including its scope, reporting system, and the competency and independence of the responsible party (this may be performed, in part or in full, by the examiner performing the review of the bank’s internal and external audit program).

Consult with the examiner assigned to the audit review and refer to the “Internal and External Audits” booklet of the *Comptroller’s Handbook*.

1. Assess the adequacy of the compliance audit function within the bank’s risk governance framework. Examiners should consider
  - independence of auditors, or the bank’s internal audit function, including reporting lines.
  - qualifications of the auditors or senior audit staff.
  - adequacy and appropriateness of the audit program.
  - degree and effectiveness of board or board committee oversight.
2. Review the bank’s documented audit plan and schedule for performing compliance audit activities. Compare the bank’s plan and schedule with audits actually performed to determine adherence to the plan and schedule. Assess the reasons for any material changes and confirm that the board reviews and approves material changes.
3. Compare the compliance risk assessment with the compliance audit plan and schedule to determine whether they correspond to the risks identified in the risk assessment.
4. Determine whether lower-risk areas are also included in the audit plan and schedule, as applicable.
5. Review audit work papers and validate that the work papers demonstrate an effective audit scope and appropriately support audit findings and conclusions.
6. Determine whether audit findings are appropriately tracked and reported to the board and management. Confirm that management’s responsiveness to correcting deficiencies is timely and effective. Verify that the audit function follows up on and validates the adequacy of management’s corrective actions to noted findings.

**Objective:** To determine whether the bank has an effective consumer complaints response and analysis process that is commensurate with its size, complexity, and risk profile and allows the board and management to identify and address trends and concerns.

1. Through review of applicable policies, procedures, and processes and discussions with management, determine whether the bank’s complaints management process appropriately
  - defines a complaint, including levels of significance or risk.
  - identifies individual(s) responsible for addressing complaints.
  - includes an escalation process for significant or high-risk complaints.
  - tracks complaints and bank responses or actions.
  - analyzes complaints to determine the root cause, or if a trend or pattern exists.
  - reports complaint data and trends to the board and management.
2. Does the bank’s process consider complaints across all products and services, business units, and affiliates, and from all channels (e.g., in person, telephone, email, litigation, regulatory, and social media)?
3. Do the bank’s complaint-related policies and procedures address how various complaints are documented and tracked?
4. Does the bank’s process incorporate internal whistleblower referrals to identify potential consumer compliance risk or consumer harm?
5. Does the bank’s process include monitoring and analyzing complaints received about and by third-party service providers?
6. Is the complaints management process centralized, or does the bank have a process to ensure that complaints received and dispositioned throughout the bank are analyzed appropriately to identify trends, patterns, and increased risk across the entire institution?
7. Review a sample of complaints and their resolutions to determine whether the bank effectively identifies complaints and provides an appropriate resolution. Refer to the “Sampling Methodologies”<sup>16</sup> booklet of the *Comptroller’s Handbook* for guidance on sampling techniques. Include complaints that suggest unfair or deceptive practices, unlawful discrimination, or other significant consumer injury.

---

<sup>16</sup> Refer to the Office of Thrift Supervision “OTS Examination Handbook” section 209, “Sampling,” regarding selecting sample sizes for examinations at federal savings associations.

## Conclusions

---

**Conclusion:** The effectiveness of the bank's consumer compliance risk management practices within its CMS is (strong, satisfactory, insufficient, or weak).

---

**Objective:** To determine, document, and communicate overall findings and conclusions regarding the examination of the bank's CMS.

1. Determine preliminary examination findings and conclusions and discuss these with the EIC or Compliance Team Lead, and other examination staff, as applicable. Provide preliminary conclusions regarding the following:
  - Quantity of associated risks (as noted in the "Introduction" section of this booklet).
  - Quality of risk management.
  - Aggregate level and direction of risk.
  - Overall risk in the bank's CMS (including compliance, operational, strategic, and reputation risk).
  - Violations and other concerns.
2. Discuss examination findings with bank management, including violations, deficient practices, and conclusions about risks and risk management practices. If necessary, obtain commitments for corrective action.
3. Assign the Consumer Compliance rating in accordance with the CC Rating System and by incorporating findings from all consumer compliance activities conducted during the supervisory cycle. Compose conclusion comments, highlighting any issues that should be included in the report of examination or supervisory letter. If necessary, compose a matters requiring attention (MRA) comment or violation write-ups. Provide the EIC or Compliance Team Lead, as applicable, with recommendations setting out what the OCC should do in the future to effectively supervise the bank's CMS, including time periods, staffing, and workdays required.
4. Update the OCC's information system and any applicable report of examination schedules or tables.
5. Update, organize, and reference work papers in accordance with OCC policy.
6. Confirm that any paper or electronic media that contain sensitive bank or customer information are appropriately disposed of or secured.

## Appendix

---

### Appendix A: Uniform Interagency Consumer Compliance Rating System (CC Rating System)

At the FFIEC’s recommendation, the federal banking regulatory agencies adopted the CC Rating System.<sup>17</sup> The rating system is meant to reflect, in a comprehensive and uniform fashion, the nature and extent of an institution’s compliance with consumer protection and civil rights statutes and regulations. The system helps identify institutions displaying compliance weaknesses requiring special supervisory attention.

The rating system provides a general framework for evaluating and integrating significant compliance factors to assign a consumer compliance rating to each institution. The rating system does not consider an institution’s record of lending performance under the CRA or its compliance with the applicable provisions of the implementing regulations. Performance with respect to the CRA is evaluated separately.

#### Overview

This CC Rating System provides a general framework for assessing risks during the supervisory process using certain compliance factors and assigning an overall consumer compliance rating to each federally regulated financial institution. The primary purpose of the CC Rating System is to ensure that regulated financial institutions<sup>18</sup> are evaluated in a comprehensive and consistent manner and that supervisory resources are appropriately focused on areas exhibiting risk of consumer harm and on institutions that warrant elevated supervisory attention. Ratings are given on a scale of 1 through 5 in increasing order of supervisory concern. 1 represents the highest rating and the lowest level of supervisory concern, while 5 represents the lowest, most critically deficient level of performance and the highest degree of supervisory concern.

The CC Rating System is composed of guidance and definitions. The guidance provides examiners with direction on how to use the definitions when assigning a consumer compliance rating to an institution. The definitions consist of qualitative descriptions for each rating category and include CMS elements reflecting risk control processes designed to manage consumer compliance risk and considerations regarding violations of laws, consumer harm, and the size, complexity, and risk profile of an institution. The consumer compliance

---

<sup>17</sup> The FFIEC issued the revised CC Rating System in November 2016 to reflect regulatory, supervisory, technological, and market changes that have occurred since the system was established in 1980. The revisions are designed to better reflect current consumer compliance supervisory approaches. The revised CC Rating System was effective for all OCC examinations that started on or after March 31, 2017. Refer to 81 Fed. Reg. 79473, “Uniform Interagency Consumer Compliance Rating System.”

<sup>18</sup> The term “financial institution” means a commercial bank, a savings bank, a trust company, a savings association, a building and loan association, a homestead association, a cooperative bank, or a credit union. Refer to 12 USC 3302(3).

rating reflects the effectiveness of an institution's CMS to ensure compliance with consumer protection laws and regulations and reduce the risk of harm to consumers.

## Categories of the Consumer Compliance Rating System

The CC Rating System is organized under three broad categories:

- Board and Management Oversight
- Compliance Program
- Violations of Law and Consumer Harm

The Consumer Compliance Rating Definitions list the assessment factors considered within each category, along with narrative descriptions of performance. The first two categories, Board and Management Oversight and Compliance Program, are used to assess a financial institution's CMS. Examiners should evaluate the assessment factors within these two categories commensurate with the institution's size, complexity, and risk profile. All institutions, regardless of size, should maintain an effective CMS. The sophistication and formality of the CMS typically increase commensurate with the size, complexity, and risk profile of the entity.

Additionally, compliance expectations contained within the narrative descriptions of these two categories extend to third-party relationships into which the financial institution has entered. There can be certain benefits to financial institutions engaging in relationships with third parties, including gaining operational efficiencies or an ability to deliver additional products and services, but such arrangements also may expose financial institutions to risks if not managed effectively. The prudential agencies, the BCFP, and some states have issued guidance describing expectations regarding oversight of third-party relationships. While an institution's management may make the business decision to outsource some or all of the operational aspects of a product or service, the institution cannot outsource the responsibility for complying with laws and regulations or managing the risks associated with third-party relationships.<sup>19</sup>

As noted in the Consumer Compliance Rating Definitions, examiners should evaluate activities conducted through third-party relationships as though the activities were performed by the institution itself. Examiners should review a financial institution's management of third-party relationships and servicers as part of its overall compliance program.

The third category, Violations of Law and Consumer Harm, includes assessment factors that evaluate the dimensions of any identified violation or consumer harm. Examiners should weigh each of these four factors—root cause, severity, duration, and pervasiveness—in evaluating relevant violations of law and any resulting consumer harm.

---

<sup>19</sup> Refer to OCC Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," OCC Bulletin 2017-21, "Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29," and OCC Bulletin 2017-7, "Third-Party Relationships: Supplemental Examination Procedures."

## Board and Management Oversight—Assessment Factors

Under Board and Management Oversight, the examiner should assess the financial institution’s board and management, as appropriate for their respective roles and responsibilities, based on the following assessment factors:

- Oversight of and commitment to the institution’s CMS.
- Effectiveness of the institution’s change management processes, including responding in a timely manner and satisfactorily to any variety of change, internal or external, to the institution.
- Comprehension, identification, and management of risks arising from the institution’s products, services, or activities.
- Self-identification of consumer compliance issues and corrective action undertaken as such issues are identified.

Table 1 lists the board and management oversight assessment factors.

**Table 1: Board and Management Oversight Assessment Factors**

<b>Board and Management Oversight</b>					
Board and management oversight factors should be evaluated commensurate with the institution’s size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.					
<b>Assessment factors</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Oversight and commitment</b>	Board and management demonstrate strong commitment to and oversight of the financial institution’s CMS.	Board and management provide satisfactory oversight of the financial institution’s CMS.	Board and management oversight of the financial institution’s CMS is deficient.	Board and management oversight, resources, and attention to the CMS are seriously deficient.	Board and management oversight, resources, and attention to the CMS are critically deficient.
	Substantial compliance resources are provided, including systems, capital, and human resources commensurate with the financial institution’s size, complexity, and risk profile. Staff is knowledgeable, empowered, and held accountable for compliance with consumer laws and regulations.	Compliance resources are adequate and staff is generally able to ensure the financial institution is in compliance with consumer laws and regulations.	Compliance resources and staff are inadequate to ensure the financial institution is in compliance with consumer laws and regulations.	Compliance resources and staff are seriously deficient and are ineffective at ensuring the financial institution’s compliance with consumer laws and regulations.	Compliance resources are critically deficient in supporting the financial institution’s compliance with consumer laws and regulations, and management and staff are unwilling or incapable of operating within the scope of consumer protection laws and regulations.

<b>Board and Management Oversight</b>					
Board and management oversight factors should be evaluated commensurate with the institution's size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.					
<b>Assessment factors</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
	Management conducts comprehensive and ongoing due diligence and oversight of third parties consistent with agency expectations to ensure that the financial institution complies with consumer protection laws, and exercises strong oversight of third parties' policies, procedures, internal controls, and training to ensure consistent oversight of compliance responsibilities.	Management conducts adequate and ongoing due diligence and oversight of third parties to ensure that the financial institution complies with consumer protection laws, and adequately oversees third parties' policies, procedures, internal controls, and training to ensure appropriate oversight of compliance responsibilities.	Management does not adequately conduct due diligence and oversight of third parties to ensure that the financial institution complies with consumer protection laws, nor does it adequately oversee third parties' policies, procedures, internal controls, and training to ensure appropriate oversight of compliance responsibilities.	Management oversight and due diligence over third-party performance, as well as management's ability to adequately identify, measure, monitor, or manage compliance risks, are seriously deficient.	Management oversight and due diligence of third-party performance are critically deficient.
<b>Change management</b>	Management anticipates and responds promptly to changes in applicable laws and regulations, market conditions, and products and services offered by evaluating the change and implementing responses across impacted lines of business.	Management responds timely and adequately to changes in applicable laws and regulations, market conditions, and products and services offered by evaluating the change and implementing responses across impacted lines of business.	Management does not respond adequately or timely in adjusting to changes in applicable laws and regulations, market conditions, and products and services offered.	Management's response to changes in applicable laws and regulations, market conditions, or products and services offered is seriously deficient.	Management fails to monitor and respond to changes in applicable laws and regulations, market conditions, or products and services offered.
	Management conducts due diligence in advance of product changes, considers the entire life cycle of a product or service in implementing change, and reviews the change after implementation to determine that actions taken have achieved planned results.	Management evaluates product changes before and after implementing the change.			

<b>Board and Management Oversight</b>					
Board and management oversight factors should be evaluated commensurate with the institution's size, complexity, and risk profile. Compliance expectations below extend to third-party relationships.					
<b>Assessment factors</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Comprehension, identification, and management of risk</b>	Management has a solid comprehension of and effectively identifies compliance risks, including emerging risks, in the financial institution's products, services, and other activities.	Management comprehends and adequately identifies compliance risks, including emerging risks, in the financial institution's products, services, and other activities.	Management has an inadequate comprehension of and ability to identify compliance risks, including emerging risks, in the financial institution's products, services, and other activities.	Management exhibits a seriously deficient comprehension of and ability to identify compliance risks, including emerging risks, in the financial institution.	Management does not comprehend or identify compliance risks, including emerging risks, in the financial institution.
	Management actively engages in managing those risks, including through comprehensive self-assessments.	Management adequately manages those risks, including through self-assessments.			
<b>Corrective action and self-identification</b>	Management proactively identifies issues and promptly responds to compliance risk management deficiencies and any violations of laws or regulations, including remediation.	Management adequately responds to and corrects deficiencies or violations, including adequate remediation, in the normal course of business.	Management does not adequately respond to compliance deficiencies and violations, including those related to remediation.	Management response to deficiencies, violations, and examination findings is seriously deficient.	Management is incapable, unwilling, or fails to respond to deficiencies, violations, or examination findings.

## Compliance Program—Assessment Factors

Under Compliance Program, the examiner should assess other elements of an effective CMS, based on the following assessment factors:

- Whether the institution's policies and procedures are appropriate to the risk in the products, services, and activities of the institution.
- The degree to which compliance training is current and tailored to risk and staff responsibilities.
- The sufficiency of the monitoring and, if applicable, audit function to encompass compliance risks throughout the institution.
- Responsiveness and effectiveness of the consumer complaint resolution process.

Table 2 lists the compliance program assessment factors.

**Table 2: Compliance Program Assessment Factors**

<b>Compliance Program</b>					
Compliance Program factors should be evaluated commensurate with the institution's size, complexity, and risk profile. Compliance expectations in this table extend to third-party relationships.					
<b>Assessment factors</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Policies and procedures</b>	Compliance policies and procedures and third-party relationship management programs are strong and comprehensive and provide standards to effectively manage compliance risk in the products, services, and activities of the financial institution.	Compliance policies and procedures and third-party relationship management programs are adequate to manage the compliance risk in the products, services, and activities of the financial institution.	Compliance policies and procedures and third-party relationship management programs are inadequate at managing the compliance risk in the products, services, and activities of the financial institution.	Compliance policies and procedures and third-party relationship management programs are seriously deficient at managing compliance risk in the products, services, and activities of the financial institution.	Compliance policies and procedures and third-party relationship management programs are critically absent.
<b>Training</b>	Compliance training is comprehensive, timely, and specifically tailored to the particular responsibilities of the staff receiving it, including those responsible for product development, marketing, and customer service.	Compliance training outlining staff responsibilities is adequate and provided in a timely manner to appropriate staff.	Compliance training is not adequately comprehensive, timely, updated, or appropriately tailored to the particular responsibilities of the staff.	Compliance training is seriously deficient in its comprehensiveness, timeliness, or relevance to staff with compliance responsibilities, or has numerous major inaccuracies.	Compliance training is critically absent.
	The compliance training program is updated proactively before the introduction of new products or new consumer protection laws and regulations to ensure that all staff are aware of compliance responsibilities before rollout.	The compliance training program is updated to encompass new products and to comply with changes to consumer protection laws and regulations.			
<b>Monitoring or audit</b>	Compliance monitoring practices, MIS, reporting, compliance audit, and internal control systems are comprehensive, timely, and successful at identifying and measuring material compliance risk management throughout the financial institution.	Compliance monitoring practices, MIS, reporting, compliance audit, and internal control systems adequately address compliance risks throughout the financial institution.	Compliance monitoring practices, MIS, reporting, compliance audit, and internal control systems do not adequately address risks involving products, services, or other activities, including timing and scope.	Compliance monitoring practices, MIS, reporting, compliance audit, and internal controls are seriously deficient in addressing risks involving products, services, or other activities.	Compliance monitoring practices, MIS, reporting, compliance audit, or internal controls are critically absent.

<b>Compliance Program</b>					
Compliance Program factors should be evaluated commensurate with the institution's size, complexity, and risk profile. Compliance expectations in this table extend to third-party relationships.					
<b>Assessment factors</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
	Programs are monitored proactively to identify procedural or training weaknesses to preclude regulatory violations. Program modifications are made expeditiously to minimize compliance risk.				
<b>Consumer complaint response</b>	Processes and procedures for addressing consumer complaints are strong. Consumer complaint investigations and responses are prompt and thorough.	Processes and procedures for addressing consumer complaints are adequate. Consumer complaint investigations and responses are generally prompt and thorough.	Processes and procedures for addressing consumer complaints are inadequate. Consumer complaint investigations and responses are not thorough or timely.	Processes and procedures for addressing consumer complaints and consumer complaint investigations are seriously deficient.	Processes and procedures for addressing consumer complaints are critically absent. Meaningful investigations and responses are absent.
	Management monitors consumer complaints to identify risks of potential consumer harm, program deficiencies, and customer service issues and takes appropriate action.	Management adequately monitors consumer complaints and responds to issues identified.	Management does not adequately monitor consumer complaints.	Management monitoring of consumer complaints is seriously deficient.	Management exhibits a disregard for complaints or preventing consumer harm.

## Violations of Law and Consumer Harm—Assessment Factors

Under Violations of Law and Consumer Harm, the examiner should analyze the following assessment factors:

- The root cause, or causes, of any violations of law identified during the examination.
- The severity of any consumer harm resulting from violations.
- The duration of time over which the violations occurred.
- The pervasiveness of the violations.

As a result of a violation of law, consumer harm may occur. While many instances of consumer harm can be quantified as a dollar amount associated with financial loss, such as charging higher fees for a product than was initially disclosed, consumer harm may also result from a denial of an opportunity. For example, a consumer could be harmed when a financial institution denies the consumer credit or discourages an application in violation of the Equal Credit Opportunity Act,<sup>20</sup> whether or not there is resulting financial harm.

<sup>20</sup> Refer to 15 USC 1691 et seq.

This category of the Consumer Compliance Rating Definitions defines four factors by which examiners can assess violations of law and consumer harm.

- **Root cause:** The root cause assessment factor analyzes the degree to which weaknesses in the CMS gave rise to the violations. In many instances, the root cause of a violation is tied to a weakness in one or more elements of the CMS. Violations that result from critical deficiencies in the CMS evidence a critical absence of management oversight and are of the highest supervisory concern.
- **Severity:** The severity assessment factor weighs the type of consumer harm, if any, that resulted from violations of law. More severe harm results in a higher level of supervisory concern under this factor. For example, some consumer protection violations may cause significant financial harm to a consumer, while other violations may cause negligible harm, based on the specific facts involved.
- **Duration:** The duration assessment factor considers the length of time over which the violations occurred. Violations that persist over an extended period of time raise greater supervisory concerns than violations that occur for only a brief period of time. When violations are brought to the attention of an institution's management and management allows those violations to remain unaddressed, such violations are of the highest supervisory concern.
- **Pervasiveness:** The pervasiveness assessment factor evaluates the extent of the violation(s) and resulting consumer harm, if any. Violations that affect a large number of consumers raise greater supervisory concern than violations that impact a limited number of consumers. If violations become so pervasive that they are considered to be widespread or present in multiple products or services, the institution's performance under this factor is of the highest supervisory concern.

Strong compliance programs are proactive. They promote consumer protection by preventing, self-identifying, and addressing compliance issues in a proactive manner. Accordingly, the CC Rating System provides incentives for such practices through the definitions associated with a 1 rating.

The agencies believe that self-identification and prompt correction of violations of law reflect strengths in an institution's CMS. A robust CMS appropriate for the size, complexity, and risk profile of an institution's business often prevents violations or facilitates early detection of potential violations. This early detection can limit the size and scope of consumer harm. Moreover, self-identification and prompt correction of serious violations represent concrete evidence of an institution's commitment to responsibly address underlying risks. In addition, appropriate corrective action, including both correction of programmatic weaknesses and full redress for injured parties, limits consumer harm, and prevents violations from recurring in the future. Thus, the CC Rating System recognizes institutions that consistently adopt these strategies as reflected in the Consumer Compliance Rating Definitions. Table 3 lists the assessment factors for violations of law and consumer harm.

**Table 3: Violations of Law and Consumer Harm Assessment Factors**

<b>Violations of Law and Consumer Harm</b>					
<b>Assessment factors to be considered</b>	<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
<b>Root cause</b>	The violations are the result of minor weaknesses, if any, in the compliance risk management system.	The violations are the result of modest weaknesses in the compliance risk management system.	The violations are the result of material weaknesses in the compliance risk management system.	The violations are the result of serious deficiencies in the compliance risk management system.	The violations are the result of critical deficiencies in the compliance risk management system.
<b>Severity</b>	The type of consumer harm, if any, resulting from the violations would have a minimal impact on consumers.	The type of consumer harm resulting from the violations would have a limited impact on consumers.	The type of consumer harm resulting from the violations would have a considerable impact on consumers.	The type of consumer harm resulting from the violations would have a serious impact on consumers.	
<b>Duration</b>	The violations and resulting consumer harm, if any, occurred over a brief period of time.	The violations and resulting consumer harm, if any, occurred over a limited period of time.	The violations and resulting consumer harm, if any, occurred over an extended period of time.	The violations and resulting consumer harm, if any, have been long-standing or repeated.	
<b>Pervasiveness</b>	The violations and resulting consumer harm, if any, are isolated in number.	The violations and resulting consumer harm, if any, are limited in number.	The violations and resulting consumer harm, if any, are numerous.	The violations and resulting consumer harm, if any, are widespread or in multiple products or services.	

## **Evaluating Performance Using the Consumer Compliance Rating Definitions (Consumer Compliance Component Rating)**

The consumer compliance rating is derived through an evaluation of the financial institution's performance under each of the assessment factors described above. The consumer compliance rating reflects the effectiveness of an institution's CMS to identify and manage compliance risk in the institution's products and services and to prevent violations of law and consumer harm, as evidenced by the financial institution's performance under each of the assessment factors.

The consumer compliance rating reflects a comprehensive evaluation of the financial institution's performance under the CC Rating System by considering the categories and assessment factors in the context of the size, complexity, and risk profile of an institution. It is not based on a numeric average or any other quantitative calculation. Specific numeric ratings will not be assigned to any of the 12 assessment factors. Thus, an institution need not achieve a satisfactory assessment in all categories in order to be assigned an overall satisfactory rating. Conversely, an institution may be assigned a less than satisfactory rating even if some of its assessments were satisfactory.

The relative importance of each category or assessment factor may differ based on the size, complexity, and risk profile of an individual institution. Accordingly, one or more category

or assessment factor may be more or less relevant at one financial institution as compared with another institution. While the expectations for compliance with consumer protection laws and regulations are the same across institutions of varying sizes, the methods for accomplishing an effective CMS may differ across institutions.

The evaluation of an institution's performance within the Violations of Law and Consumer Harm category of the CC Rating Definitions considers each of the four assessment factors: root cause, severity, duration, and pervasiveness. At the levels of 4 and 5 in this category, the distinctions in the definitions are focused on the root cause assessment factor rather than severity, duration, and pervasiveness. This approach is consistent with the other categories where the difference between a 4 and a 5 is driven by the institution's capacity and willingness to maintain a sound consumer compliance system.

In arriving at the final rating, the examiner must balance potentially differing conclusions about the effectiveness of the financial institution's CMS over the individual products, services, and activities of the organization. Depending on the relative materiality of a product line to the institution, an observed weakness in the management of that product line may or may not impact the conclusion about the institution's overall performance in the associated assessment factor(s). For example, serious weaknesses in the policies and procedures or audit program of the mortgage department at a mortgage lender would be of greater supervisory concern than those same gaps at an institution that makes very few mortgage loans and strictly as an accommodation. Greater weight should apply to the financial institution's management of material products with significant potential consumer compliance risk.

An institution may receive a less than satisfactory rating even when no violations were identified, based on deficiencies or weaknesses identified in the institution's CMS. For example, examiners may identify weaknesses in elements of the CMS in a new loan product. Because the presence of those weaknesses left unaddressed could result in future violations of law and consumer harm, the CMS deficiencies could impact the overall consumer compliance rating, even if no violations were identified.

Similarly, an institution may receive a 1 or 2 rating even when violations were present, if the CMS is commensurate with the risk profile and complexity of the institution. For example, when violations involve limited impact on consumers, were self-identified, and resolved promptly, the evaluation may result in a 1 or 2 rating. After evaluating the institution's performance in the two CMS categories, Board and Management Oversight and Compliance Program, and the dimensions of the violations in the third category, the examiner may conclude that the overall strength of the CMS and the nature of observed violations viewed together do not present significant supervisory concerns. Table 4 lists the consumer compliance component rating definitions.

**Table 4: Consumer Compliance Ratings**

<b>1</b>	The highest rating of 1 is assigned to a financial institution that maintains a strong CMS and takes action to prevent violations of law and consumer harm.
<b>2</b>	A rating of 2 is assigned to a financial institution that maintains a CMS that is satisfactory at managing consumer compliance risk in the institution's products and services and at substantially limiting violations of law and consumer harm.
<b>3</b>	A rating of 3 reflects a CMS deficient at managing consumer compliance risk in the institution's products and services and at limiting violations of law and consumer harm.
<b>4</b>	A rating of 4 reflects a CMS seriously deficient at managing consumer compliance risk in the institution's products and services or at preventing violations of law and consumer harm. "Seriously deficient" indicates fundamental and persistent weaknesses in crucial CMS elements and severe inadequacies in core compliance areas necessary to operate within the scope of statutory and regulatory consumer protection requirements and to prevent consumer harm.
<b>5</b>	A rating of 5 reflects a CMS critically deficient at managing consumer compliance risk in the institution's products and services or at preventing violations of law and consumer harm. "Critically deficient" indicates an absence of crucial CMS elements and a demonstrated lack of willingness or capability to take the appropriate steps necessary to operate within the scope of statutory and regulatory consumer protection requirements and to prevent consumer harm.

## Assignment of Ratings by Supervisor(s)

The prudential regulators continue to assign and update, as appropriate, consumer compliance ratings for institutions they supervise, including those with total assets of more than \$10 billion.<sup>21</sup> As an FFIEC member, the BCFP also uses the CC Rating System to assign a consumer compliance rating, as appropriate, for institutions with total assets of more than \$10 billion, as well as for nonbanks for which the BCFP has jurisdiction regarding the enforcement of federal consumer financial laws as defined under Dodd–Frank.<sup>22</sup> The prudential regulators take into consideration any material supervisory information provided by the BCFP, as that information relates to covered supervisory activities or covered examinations.<sup>23</sup> Similarly, the BCFP takes into consideration any material supervisory information provided by prudential regulators in appropriate supervisory situations.

<sup>21</sup> Section 1025 of Dodd–Frank (12 USC 5515) applies to federally insured institutions with more than \$10 billion in total assets. This section granted the BCFP exclusive authority to examine insured depository institutions and their affiliates for compliance with federal consumer financial laws. The prudential regulators retained authority for examining insured depository institutions with more than \$10 billion in total assets for compliance with certain other laws related to consumer financial protection, including the Fair Housing Act, SCRA, and section 5 of the Federal Trade Commission Act.

<sup>22</sup> Refer to 12 USC 5481 et seq., "Definitions." A financial institution with assets over \$10 billion may receive a consumer compliance rating by both its primary prudential regulator and the BCFP. The rating is based on each agency's review of the institution's CMS and compliance with the federal consumer protection laws falling under each agency's jurisdiction.

<sup>23</sup> The prudential regulators and the BCFP signed a Memorandum of Understanding on Supervisory Coordination dated May 16, 2012, intended to facilitate the coordination of supervisory activities involving financial institutions with more than \$10 billion in assets as required under Dodd–Frank.

## References

---

### Laws

- 12 USC 2801 et seq., “Home Mortgage Disclosure Act of 1975”
- 12 USC 2901 et seq., “Community Reinvestment Act of 1977”
- 12 USC 3301 et seq., “Federal Financial Institutions Examination Council Act of 1978”
- 15 USC 1691 et seq., “Equal Credit Opportunity Act”
- 42 USC 3601 et seq., “Fair Housing Act”
- 50 USC 3901 et seq., “Servicemembers Civil Relief Act”

### Regulations

- 12 CFR 30, appendix A, “Interagency Guidelines Establishing Standards for Safety and Soundness”
- 12 CFR 30, appendix D, “OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches”
- 12 CFR 1003, “Home Mortgage Disclosure Act” (Regulation C)

### Comptroller’s Handbook

#### Examination Process

- “Bank Supervision Process”
- “Community Bank Supervision”
- “Federal Branches and Agencies Supervision”
- “Large Bank Supervision”
- “Sampling Methodologies”<sup>24</sup>

#### Safety and Soundness, Management

- “Corporate and Risk Governance”
- “Internal and External Audits”

### OCC Issuances

#### OCC Bulletins

- OCC Bulletin 2013-29, “Third-Party Relationships: Risk Management Guidance” (October 30, 2013)
- OCC Bulletin 2014-45, “Heightened Standards for Larger Banks; Integration of 12 CFR 30 and 12 CFR 170: Final Rules and Guidelines” (September 25, 2014)

---

<sup>24</sup> Refer to the “OTS Examination Handbook” section 209, “Sampling,” regarding selecting sample sizes for examinations at federal savings associations.

OCC Bulletin 2017-7, “Third-Party Relationships: Supplemental Examination Procedures” (January 24, 2017)

OCC Bulletin 2017-21, “Third-Party Relationships: Frequently Asked Questions to Supplement OCC Bulletin 2013-29” (June 7, 2017)

OCC Bulletin 2017-43, “New, Modified, or Expanded Bank Products and Services: Risk Management Principles” (October 20, 2017)

### **OCC News Releases**

OCC News Release 2012-85, “Memorandum of Understanding on Supervisory Coordination” (June 4, 2012)

## **FFIEC Issuances**

“A Guide to HMDA Reporting: Getting It Right!”

## **Federal Register**

81 Fed. Reg. 79473, “Uniform Interagency Consumer Compliance Rating System” (November 14, 2016)