Compliance Management Review – Information Technology (CMR-IT)

Exam Date:	[Click&type]
Exam ID No.	[Click&type]
Prepared By:	[Click&type]
Reviewer:	[Click&type]
Supervision ID #:	[Click&type]
Entity Name:	[Click&type]
Event #:	[Click&type]

General Principles and Introduction

Institutions[1] within the scope of the CFPB's supervision and enforcement authority include both depository institutions and non-depository consumer financial services companies. These institutions operate in a dynamic environment influenced by challenges to profitability, increased focus on outcomes to consumers, industry consolidation, advancing technology, market globalization, and changes to laws and regulations.

To remain competitive and responsive to consumer needs in such an environment, institutions continuously assess their business strategies and modify product and service offerings and delivery channels. To maintain legal compliance, an institution should develop and maintain a sound compliance management system (CMS) that is integrated into the overall framework for product design, delivery, and administration across its entire product and service life cycle. Ultimately, compliance should be part of the day-to-day responsibilities of management and the employees of a supervised entity. Issues should be self-identified, and corrective action should be initiated by the entity. Institutions are also expected to manage relationships with service providers to ensure that service providers effectively manage compliance with Federal consumer financial laws applicable to the product or service being provided.[2]

Institutions often use information technology (IT) that could impact compliance with Federal consumer financial laws. As part of its overall CMS assessment, the CFPB may evaluate the technology controls of an institution and its service providers. The CFPB may also evaluate an institution's IT as it relates to compliance with Federal consumer financial laws. The Compliance Management System – Information Technology (CMS-IT) examination procedures set forth below are used by examiners to assess IT and IT controls as part of a CMS review.

A CMS is how an institution:

- Establishes its compliance responsibilities;
- Communicates those responsibilities to employees;
- Ensures that responsibilities for meeting legal requirements and internal policies and procedures are incorporated into business processes;

[1] The terms "institution" and "entity" are used interchangeably throughout this document.

[2] See CFPB Bulletin 2016-02, Service Providers (October 31, 2016), which describes the CFPB's expectation that supervised banks and nonbanks oversee their business relationships with service providers in a manner that ensures compliance with Federal consumer financial law. Compliance Bulletin and Policy Guidance; 2016-02

- Reviews operations to ensure responsibilities are carried out and legal requirements are met; and
- Takes corrective action and updates tools, systems, and materials as necessary.

An effective CMS commonly has two interdependent control components:

- Board and Management Oversight; and
- Compliance Program, which includes:
  - Policies and procedures;
  - Training;
  - Monitoring and/or audit; and
  - Consumer complaint response.

When the two interdependent control components are strong and well-coordinated, an institution typically is successful at managing its compliance responsibilities and risks.

Additionally, the Bureau's supervisory expectations with respect to an institution's compliance program extend to service provider relationships into which the institution has entered. There can be certain benefits to institutions engaging in relationships with service providers, including gaining operational efficiencies or an ability to deliver additional products and services. However, such arrangements may also expose institutions to risks when not managed properly. 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 Federal consumer financial laws or managing the risks associated with service provider relationships.

Weaknesses in a CMS can result in violations of Federal consumer financial law and associated harm to consumers. Therefore, the CFPB expects every institution under its supervision and enforcement authority to have a CMS adapted to its business strategy and operations. The CFPB understands that compliance will likely be managed differently by large banking organizations with complex compliance profiles and a wide range of consumer financial products and services[3] at one end of the spectrum, than by non-bank entities that may be owned by a single individual and feature a narrow range of financial products and services, at the other end of the spectrum. Compliance may be managed on an enterprise-wide basis, and institutions may engage outside firms to assist with compliance management. However compliance is managed, a provider of consumer financial products or services under CFPB's supervisory purview is expected to comply with Federal consumer financial laws and appropriately address and limit violations of law and associated harms to consumers.

[3] For example, the Federal Reserve Board of Governors expects large banking organizations with complex compliance profiles to implement firm-wide compliance risk management programs and have a corporate compliance function. SR 08-8 / CA 08-11, October 16, 2008. The CFPB will expect no less.

The CFPB also understands that institutions will organize their CMS to include compliance with consumer-related state and Federal laws that are outside the scope of the CFPB's supervision responsibilities, in addition to the matters that are within the CFPB's scope. The CFPB, therefore, expects that CMS be organized within a firm, legal entity, division, or business unit in the way that is most effective to the institution, and that the manner of organization will vary from institution to institution.

This CMS examination manual is divided into five Modules:

- Module 1: Board and Management Oversight
- Module 2: Compliance Program
- Module 3: Service Provider Oversight
- Module 4: Violations of Law and Consumer Harm
- Module 5: Examiner Conclusions and Wrap-Up

Module 1: Board and Management Oversight

In a depository institution, the board of directors is ultimately responsible for developing and administering a CMS that ensures compliance with Federal consumer financial laws and addresses and minimizes associated risks of harm to consumers. In a non-depository consumer financial services company, that ultimate responsibility may rest with a board of directors in the case of a corporation or with a controlling person or some other arrangement. For the balance of this section of the Manual, references to the "board of directors" or "board" generally refer to the board of directors or other individual or group exercising similar oversight functions. In addition, some institutions may be governed by firm-wide standards, policies, and procedures developed by a holding company or other top-tier corporation for adoption, use, and modification, as necessary, by subsidiary entities.

In the absence of a board of directors and board committee structure, the examiner should determine that the person or group exercising similar oversight functions receives relevant information about compliance and consumer protection matters and takes steps to ensure that the key elements, resources, and individuals necessary for a CMS commensurate with the supervised entity's risk profile are in place and functioning.

Under Board and Management Oversight, examiners should assess the institution's board of directors and management, as appropriate, for their respective roles and responsibilities, based on the following 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; and
- Self-identification of consumer compliance issues and corrective action undertaken as such issues are identified.

Board and Management Oversight – Examination Objectives

Since the effectiveness of a CMS is grounded in the actions taken by its board and senior management, examiners should seek to determine whether the board and management meet the following objectives:

Oversight of and Commitment to the Institution's CMS

1. Demonstrate a strong commitment and oversight to the institution's CMS.
2. Provide compliance resources including systems, capital, and human resources commensurate with the institution's size, complexity, and risk profile.
3. Ensure that staff is knowledgeable, empowered and held accountable for compliance with Federal consumer financial laws.
4. Conduct comprehensive and ongoing due diligence and oversight of service providers consistent with the CFPB's expectations to ensure that the institution complies with Federal consumer financial laws.
5. Exercise oversight of service providers' policies, procedures, internal controls, and training to ensure consistent oversight of compliance responsibilities.

Change Management

1. Respond promptly to changes in applicable Federal consumer financial laws, market conditions, and products and services offered by evaluating the change and implementing responses across impacted lines of business.
2. Conduct due diligence in advance of product changes, consider the entire life cycle of a product or service in implementing change and review the change after implementation to determine whether the actions taken achieved the planned results.

Comprehension, Identification and Management of Risk

1. Comprehend and identify compliance risks, including emerging risks, in the institution's products, services, and other activities.
2. Engage themselves in managing identified risks, which include using comprehensive self-assessments and independent audits, as applicable.
3. Address consumer compliance issues and associated risks of harm to consumers throughout product development, marketing, and account administration, and through the entity's handling of consumer complaints and inquiries.

Self-Identification and Corrective Action

1. Proactively identify issues.

2. Promptly respond to CMS deficiencies and any violations of laws or regulations, including remediation.

Board and Management Oversight – IT Examination Procedures

1. Review board meeting minutes and supporting materials during the period under review for coverage of IT and IT controls that may impact compliance with Federal consumer financial law.

[Click&type]

2. Determine board and management's oversight and review of the IT function (e.g., board meeting minutes, strategic plan, significant initiatives or changes).

[Click&type]

3. Assess the compliance and IT organizational structures, including:

    a. Direct reporting line from IT management to senior level management;

    b. Appropriate separation of duties between business functions and IT functions;

    c. Appropriate separation of duties within the IT function;

    d. Coordination and reporting line between IT management and compliance management; and

    e. Board and management committee structures (responsibility and authority).

[Click&type]

4. Determine the existence of a board approved, comprehensive information security program.

[Click&type]

5. Determine whether the board or a sub-committee of the board reviews the IT risk management process, including risk identification, risk assessment, and risk mitigation. Further, determine whether management has developed adequate policies, standards, and procedures to manage technology risk and whether they are current, documented, and appropriately communicated. Determine whether compliance with Federal consumer financial laws is incorporated into the risk process and associated documentation.

[Click&type]

6. Determine whether the board and management oversee changes or anticipated changes in technology enterprise-wide (e.g., service provider relationships, software applications, and/or service offerings).

[Click&type]

7. Determine if management has identified all information assets and systems, including cloud-based and virtualized systems as well as critical service providers that are related to consumer financial services and/or products.

[Click&type]

8. Determine whether the board and management evaluate whether written policies, control procedures, and standards are thorough, properly reflect the complexity of the IT environment, and incorporate compliance with Federal consumer financial laws. Also, evaluate whether these policies, control procedures, and standards have been formally adopted, communicated, and enforced.

[Click&type]

9. Determine if the board and management consider whether inherent risks related to IT have been evaluated, including impact to consumers; controls have been clearly identified; and residual risks are at acceptable levels.

[Click&type]

10. Determine whether the entity's risk assessment program, including IT-related risk, has been formally approved by the board of directors.

[Click&type]

11. Determine whether a report of risk assessment findings, including IT-related risk, has been presented to the board of directors for review.

[Click&type]

12. Determine whether board and management evaluate the adequacy of short- and long-term IT strategic planning and resource allocation.

[Click&type]

13. Determine whether board and management oversee the controls around the system development life cycle (SDLC), including the integration of compliance with Federal consumer financial laws into the SDLC process, and whether that is appropriate for the size and complexity of the entity.

[Click&type]

14. Determine whether senior management oversees the IT change management process that aligns with the entity's IT risk appetite. Further, determine whether management has developed adequate policies, standards, and procedures to address change management for applications or systems used to support compliance with Federal consumer financial laws.

[Click&type]

15. Determine whether the board has established an ongoing, process-oriented approach to business continuity planning that is appropriate for the size and complexity of the entity.

[Click&type]

16. Determine whether management implements and uses IT system reporting and whether it produces accurate and useful reports. Determine the effectiveness of the reports used by senior management or relevant management committees to supervise and monitor the IT functions.

[Click&type]

17. Draw preliminary conclusions as to whether board and senior management oversight related to IT is strong, satisfactory, deficient, seriously deficient, or critically deficient. Further, include how IT oversight impacts compliance with Federal consumer financial laws.

[Click&type]

Module 2: Compliance Program

A sound Compliance Program is essential to the efficient and successful operation of the supervised entity. A Compliance Program includes the following components:

- Policies and procedures;
- Training;
- Monitoring and/or audit; and
- Consumer complaint response.

An institution should establish a formal, written Compliance Program, and that program generally should be administered by a chief compliance officer. In addition to being a planned and organized effort to guide the entity's compliance activities, a written program represents an essential source document that may serve as a training and reference tool for employees. A well-planned, implemented, and maintained Compliance Program may prevent or reduce regulatory violations,

protect consumers from non-compliance and associated harms, and help align business strategies with outcomes. The examination objectives and procedures for the Compliance Program are divided in this module among the four components.

Policies and Procedures – Examination Objectives

Compliance policies and procedures should document and be sufficiently detailed to implement the board-approved policy documents. Examiners should seek to determine whether compliance policies and procedures:

1. Are designed to effectively manage IT controls and compliance risk in the products, services and activities of the institution.
2. Are consistent with board-approved compliance policies.
3. Address compliance with applicable Federal consumer financial laws in a manner designed to minimize violations and to detect and minimize associated risks of harm to consumers.
4. Cover the full life cycle of all IT products (e.g., software programs, systems, and components) and/or services offered.
5. Are maintained and modified to remain current and complete, and to serve as a reference for employees in their day-to-day activities.

Policies and Procedures – IT Examination Procedures

1. Review and understand how the consumer compliance program is structured and how it interacts with IT functions and controls to ensure compliance with Federal consumer financial laws.

[Click&type]

2. Review policies and procedures pertaining to the creation and maintenance of IT policies and procedures.

[Click&type]

3. Request and review IT policies and procedures that may impact compliance with Federal consumer financial laws.

[Click&type]

4. Review IT policies and procedures to determine whether and how they address new or amended Federal consumer financial laws.

[Click&type]

5. Determine whether the entity follows IT policies and procedures, including a system development life cycle (SDLC) which integrates compliance with Federal consumer financial laws where applicable, when developing systems to support new products or services.

[Click&type]

6. Determine if IT policies and procedures maintained by different regional, business unit, or legal entities are consistent with applicable corporate or board-level policies. If any inconsistencies are noted, determine if they are justified by business necessity or market condition.

[Click&type]

7. Review IT procedures related to record retention and destruction timeframes for compliance with related internal policies and legal requirements.

[Click&type]

8. Draw preliminary conclusions as to whether IT policies and procedures are strong, satisfactory, deficient, seriously deficient, or critically deficient. Further, include how IT policies and procedures may impact compliance with Federal consumer financial laws.

[Click&type]

Training – Examination Objectives

Education of an entity's board of directors, management, and staff is essential to maintaining an effective compliance program. Board members should receive sufficient information to enable them to understand the entity's responsibilities and the commensurate resource requirements. Management and staff should receive specific, comprehensive training that reinforces and helps support written policies and procedures. Requirements for compliance with Federal consumer financial laws, including prohibitions against unlawful discrimination and unfair, deceptive, and abusive acts and practices, should be incorporated into training for all relevant officers and employees, including audit and applicable IT personnel. Examiners should seek to determine whether:

1. Training is comprehensive, timely, and specifically tailored to the particular responsibilities of the staff receiving it.

2. The training program is updated proactively in advance of the rollout of new or changed products or the effective date of new or changed consumer protection laws and regulations to ensure that all staff is aware of compliance responsibilities.

3. Training is consistent with policies and procedures and designed to reinforce those policies and procedures.

4. Compliance and IT professionals have access to training that is necessary to administer programs that are tailored to the supervised entity's risk profile, business strategy, and operations.

Training – IT Examination Procedures

1. Request and review the schedule, record of completion, and materials for recent security awareness training of all employees, including executive officers, contractors, and board members.

[Click&type]

2. Request and review policies, schedules, training content, and records of completion for IT role-based training of IT staff. In addition, request and review documents demonstrating that service providers with IT responsibilities are appropriately trained.

[Click&type]

3. Determine the involvement of management in selecting, reviewing, or delivering IT training content. Review IT training developed as a result of management commitments to address monitoring, audit, or examination findings and recommendations or issues raised in consumer complaints and inquires.

[Click&type]

4. Review records of follow-up, escalation, and enforcement for IT staff training completion rates that do not meet the supervised entity's standards or deadlines.

[Click&type]

5. Request and review the entity's plans for additions, deletions, or modifications to IT training over the next 12 months and compare actual training activities to prior plans.

[Click&type]

6. Draw preliminary conclusions as to whether the IT training program is strong, satisfactory, deficient, seriously deficient, or critically deficient.

[Click&type]

Monitoring and/or Audit – Examination Objectives

Monitoring is a compliance program element that seeks to identify CMS weaknesses by promptly identifying and correcting weaknesses. Monitoring is generally more frequent and less formal than audit, may be carried out by the business unit, and does not require the same level of independence from the business or compliance function that an audit program requires.

Conversely, audit is generally less frequent and more formal than monitoring, may be carried out by an institution's internal audit department or outside contracted party, and is generally independent of the business or compliance function that does the monitoring.

The audit function should review an institution's compliance with Federal consumer financial laws and adherence to internal policies and procedures, and it should be independent of both the compliance program and business functions. IT and compliance audit programs provide the board of directors, or its designated committees, with a determination of whether policies and procedures adopted by the board to guide risk management are being implemented and followed to provide for the level of compliance and consumer protection established by the board.

Examiners should evaluate monitoring and audit programs to determine whether they are commensurate with the institution's size, complexity, and risk profile. In some instances, particularly in institutions that are small, are non-complex in their organizational or operational structure, and that engage in products and services that present low risk of consumer harm, it is possible that the institution's CMS only has one of these functions. In instances where an institution does not have both functions, examiners should evaluate whether coverage is commensurate with the institution's size, complexity, and risk profile.

Examiners' review of compliance monitoring and/or audit should determine whether:

1. Compliance monitoring practices, management information systems, reporting, compliance audit, and internal control systems, including IT controls, are comprehensive, timely, and successful at identifying and measuring material compliance risk management throughout a specific product line and/or the institution.

2. Programs are monitored proactively to identify procedural or training weaknesses to mitigate regulatory violations. Program modifications are made timely to minimize compliance risk.

3. The institution is determining that financial services, transactions, and other consumer engagements supported by IT systems are handled according to the entity's policies and procedures.

4. Monitoring considers the results of risk assessments or other guides for prioritizing reviews.

5. Findings resulting from monitoring reviews are escalated to management and to the board of directors, as appropriate.

6. The audit program is sufficiently independent and reports to the board or a committee of the board.

7. The audit program addresses compliance with all applicable Federal consumer financial laws.

8. The schedule and coverage of audit activities is appropriate for the institution's size, complexity, risk profile; consumer financial product offerings; and manner of conducting its consumer financial products business.

9. All appropriate compliance and business unit managers receive copies of audit reports in a timely manner.

Monitoring and/or Audit –IT Examination Procedures

1. Determine whether management has Quality Assurance (QA) and Quality Control (QC) procedures defined for significant IT activities and whether those procedures are performed internally or externally.

[Click&type]

2. Review policies and procedures pertaining to IT audit.

[Click&type]

3. Evaluate the independence of the monitoring and/or audit function and the degree to which it identifies and reports weaknesses and risks to the board of directors or its audit committee. Determine whether auditor expertise and training is sufficient for the complexity of the IT function in relation to the technology and overall risk at the entity.

[Click&type]

4. If IT monitoring and/or audit is performed by a third party, request and review the applicable policy, engagement letters, and contracts covering the review period.

[Click&type]

5. Evaluate the quality of IT audit oversight and support provided by the board of directors and management. Include an evaluation of the board and management's approved risk assessment process to ensure IT audit plans address all significant IT functions.

[Click&type]

6. Determine whether monitoring and/or audit coverage includes assessment of IT system capabilities and compliance with Federal consumer financial laws and regulations, including information security controls related to consumer compliance.

[Click&type]

7. Evaluate the entity's audit coverage of user and system access. Ensure the audit covers access restrictions, unauthorized access, the number of employees requiring access, and the different types of access (i.e., logical or physical).

[Click&type]

8. Determine if the entity adjusts risk assessments in response to IT audit and monitoring results.

[Click&type]

9. Evaluate the process for ensuring IT monitoring, audit, and/or related regulatory findings are fully remediated or mitigated.

[Click&type]

10. Draw preliminary conclusions as to whether the IT monitoring and/or audit function is strong, satisfactory, deficient, seriously deficient, or critically deficient. Further, include how the IT monitoring and/or audit function impacts compliance with Federal consumer financial laws.

[Click&type]

Consumer Complaint Response – Examination Objectives

An effective CMS should ensure that an institution is responsive and responsible in handling consumer complaints and inquiries. Intelligence gathered from consumer contacts should be organized, retained, and used as part of an institution's CMS. The institution should be making a deliberate, good faith effort toward resolution of each consumer complaint.

Examiners will consider consumer complaints to determine the responsiveness and effectiveness of the consumer complaint resolution process. Examiners will assess whether:

1. Processes and procedures for addressing consumer complaints are appropriate.
2. Consumer complaint investigations and responses are reasonable.
3. Consumer complaints and inquiries, regardless of the channel through which they are submitted, are appropriately recorded and categorized.
4. Consumer complaints and inquiries, whether regarding the entity or its service providers, are addressed and resolved promptly.
5. Consumer complaints that raise legal issues involving potential consumer harm from unfair treatment or discrimination, unauthorized product enrollment, account openings or upgrades (including the addition of ancillary products), improper sales practices, imminent foreclosures, or other regulatory compliance issues, are appropriately categorized and escalated.
6. Management monitors consumer complaints to identify risks of potential consumer harm and CMS deficiencies, including risks to consumers for which IT issues may be the root cause, and takes appropriate prospective and retrospective corrective action.

7. Consumer complaints result in retrospective corrective action to correct the effects of the supervised entity's actions when appropriate.

8. The nature or number of substantive complaints from consumers indicates that potential weaknesses in the CMS exist.

Consumer Complaint Response – IT Examination Procedures

1. Obtain and review IT-related consumer complaints and inquiries about the entity and its service providers.

[Click&type]

2. Determine whether the entity's policies and procedures for receiving, escalating, and resolving IT issues from consumer complaints and inquiries are adequate for the entity's size, complexity, and risk profile.

[Click&type]

3. Evaluate the entity's responses, corrective actions, analysis, and categorization of IT-related consumer complaints and inquiries.

[Click&type]

4. Determine whether corrective action is offered or taken for any IT-related complaint resulting in a conclusion of violation of law or regulation.

[Click&type]

5. Draw preliminary conclusions as to whether the supervised entity's response to IT-related consumer issues and concerns is strong, satisfactory, deficient, seriously deficient, or critically deficient.

[Click&type]

Module 3: Service Provider Oversight

The CFPB recognizes that the use of service providers is often an appropriate business decision for institutions. Institutions may outsource certain functions to service providers due to resource constraints, or expertise constraints.

The fact that an institution enters into a business relationship with a service provider, however, does not negate the institution's responsibility in complying with Federal consumer financial law. A service provider that is unfamiliar with the legal requirements applicable to the products or services being offered, or that does not make efforts to implement those requirements carefully and effectively, or that exhibits weak internal controls, can harm consumers and create

potential liabilities for both the service provider and the entity with which it has a business relationship. Depending on the circumstances, legal responsibility may lie with the institution as well as with the supervised service provider.

Service Provider Oversight – Examination Objectives

Examiners should determine whether institutions have met the following expectations regarding service provider oversight:

1. The institution has developed and implemented an appropriate risk management program for service providers based on the size, scope, complexity, importance, and potential for consumer harm.

2. The institution's service provider risk management program includes initial and ongoing due diligence reviews to verify that the service provider understands and is capable of complying with Federal consumer financial law.

3. The institution ensures that the service provider conducts appropriate training and oversight of employees or agents that have consumer contact or compliance responsibilities.

4. The institution has included in its contract with the service provider clear expectations about compliance, as well as appropriate and enforceable consequences for violating any compliance-related responsibilities, including engaging in discrimination and unfair, deceptive, or abusive acts or practices.

5. The institution has established internal controls and ongoing monitoring to determine whether the service provider is complying with Federal consumer financial law.

6. The institution takes prompt action to fully address any problems identified through the monitoring process, including terminating the relationship where appropriate.

Service Provider Oversight –IT Examination Procedures

1. Determine whether and to what extent the entity uses service providers to support IT functions that could have implications for compliance with Federal consumer financial laws.

[Click&type]

2. Request and review the entity's risk management program for service providers that support IT functions that could have consumer compliance implications.

[Click&type]

3. For critical service providers with access to sensitive customer information, evaluate the entity's assessment of these service providers' written information security programs.

[Click&type]

4. Determine whether the entity maintains policies and procedures related to application or system acquisition activities where the application or system is used to support compliance with Federal consumer financial laws. This includes the project management standards, methodologies, and practices for application development.

[Click&type]

5. Determine whether the entity has policies, procedures, and processes in place to take prompt corrective action to fully address changes or conversions to service provider information systems, as well as any problems identified through the monitoring process, including termination, when appropriate.

[Click&type]

6. Where indicated by the risk assessment, determine whether management reviews IT audit summaries, test results, and other equivalent evaluations of their service providers to confirm that they are fulfilling contractual obligations.

[Click&type]

7. Determine if the entity has formal service level agreements with all of its third-party providers and if the agreements include assurance of continued service.

[Click&type]

8. Draw preliminary conclusions as to whether the institution's service provider oversight is strong, satisfactory, deficient, seriously deficient, or critically deficient. Consider the impact that this conclusion has on conclusions regarding Board and Management Oversight and components contained within the Compliance Program.

[Click&type]

Module 4: Violations of Law and Consumer Harm

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 an institution denies the consumer credit or discourages an application in violation of the Equal Credit Opportunity Act.

When violations and consumer harm are identified, it is important for examiners to consider whether the institution's CMS identified the violation and implemented appropriate corrective action. Self-identification and correction of violations of law reflect strengths in an institution's CMS. A CMS appropriate for the size, complexity and risk profile of an institution's business often will minimize violations or will facilitate early detection of potential violations. This early detection can limit the size and scope of consumer harm. Moreover, self-identification and

corrective action on serious violations represents evidence of an institution's commitment to responsibly address underlying risks. 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.

Violations of Law and Consumer Harm – Examination Objectives

In the event that examiners identify violations of Federal consumer financial law, they should consider the following factors:

1. The root cause of the violation: the degree to which weaknesses in the CMS contributed to the violation(s) of Federal consumer financial law. In many instances, the root cause of a violation may be 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.

2. The severity of consumer harm: the type of harm, if any, that resulted from the violation(s) of Federal consumer financial law. More severe harm results in a higher level of supervisory concern. For example, some violations may cause significant financial harm to a consumer, while other violations may cause negligible harm, based on the specific facts involved.

3. The duration of the violation: the length of time over which the violation(s) of Federal consumer financial law occurred. Violations that persist over an extended period of time will 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.

4. The pervasiveness of the violations: the extent of the violation(s) of Federal consumer financial law and resulting consumer harm, if any. Violations that affect a large number of consumers will 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 is of the highest supervisory concern.

Violations of Law and Consumer Harm – Examination Procedures

The following examination procedures should be conducted in the event that Examiners note violations of Federal consumer financial law:

1. Determine the root cause of the violation(s) by identifying the weaknesses in the institution's CMS that contributed to the noted violations(s). Review preliminary conclusions drawn from Modules 1, 2, and 3 on the component(s) identified as the root cause and revise those conclusions accordingly, keeping in mind that not all violations of law indicate weaknesses in CMS.

[Click&type]

2. Determine whether the institution self-identified violation(s) and consumer harm and assess the effectiveness of any corrective action implemented as a result.

[Click&type]

3. Draw a conclusion as to whether the violations are a result of minor weaknesses, modest weaknesses, material weaknesses, serious deficiencies, or critical deficiencies in the CMS.

[Click&type]

4. Assess the severity of the consumer harm that resulted from the violations(s) by determining the degree of impact that the violation has on consumers. Consider the degree of financial impact or impact of non-financial harm.

[Click&type]

5. Draw a conclusion as to whether the type of harm resulting from the violation(s) would have a minimal, limited, considerable, or serious impact on consumers.

[Click&type]

6. Assess the duration of the violation(s) and resulting consumer harm by determining the time period over which the violation occurred. Consider whether management was aware of the violation(s) and whether they took action to resolve the issue or allowed it to continue.

[Click&type]

7. Determine the pervasiveness of the violation(s) and consumer harm by considering the number of affected consumers. Consider whether the violation(s) and consumer harm are limited or whether they are widespread or in multiple products or services.

[Click&type]

Module 5: Examiner Conclusions and Wrap-Up

To conclude this supervisory activity, examiners must complete all the steps under this section, regardless of the entity's risk profile:

1. Summarize the findings, supervisory concerns and conclusions for each Module completed.

[Click&type]

2. Identify action needed to correct weaknesses in the institution's CMS.

[Click&type]

3. Discuss findings with the institution's management and, if necessary, obtain a commitment for corrective action.

[Click&type]

4. Record findings according to Bureau policy in the Examination Report/Supervisory Letter.

[Click&type]

5. Prepare a memorandum for inclusion in the work papers and CFPB's official system of record that outlines planning and strategy considerations for the next examination and, if appropriate, interim follow-up.

[Click&type]