Table of Contents

3.2 Compliance Program

[Sample Client]'s compliance program is multi-faceted to ensure compliance personnel are integral company stakeholders to successfully identify areas of high risk and prioritize the CMS components around those risks.

[Sample Client]'s compliance program includes the following:

- Policies and procedures
- Compliance training
- Monitoring and/or auditing
- Consumer complaint response

[Sample Client] has a formal, written compliance program, administered by compliance personnel whose experience and qualifications are commensurate with their roles and responsibilities. [Sample Client]'s written program is a planned and organized guide for compliance activities and serves as an essential source document for employee reference and training.

3.2.1 Policies and Procedures

[Sample Client]'s compliance program is designed to manage policies and procedures both internally and externally. Internally the compliance program ensures [Sample Client]'s policies and procedures are sufficiently detailed to implement the board-approved compliance policies and effectively mitigate compliance. [Sample Client] also reviews the policies and procedures of their third-party service providers to assess if the regulatory risk associated with their specific products and services are effectively mitigated.

[Sample Client]'s compliance program is designed to ensure compliance with policies and procedures as follows:

- Effectively manage IT controls and compliance risks in the products, services, and activities associated with the origination and servicing of residential mortgage loans
- Are consistent with board-approved compliance policies and structured to ensure they meet the board's expectations
- Address compliance with applicable consumer protection-related laws and regulations to minimize violations and actively detect and minimize associated risks of harm to consumers
- Cover the full life cycle of all products and services offered, including IT products, such as software programs, systems, and components

Risk Tolerance

Risk tolerance statements establish the acceptable minimum and maximum levels of [Sample Client]'s tolerance to identified risks. Compliance risk tolerance levels are at or near zero.

Key Risk Indicators (KRIs)

[Sample Client] utilizes KRI metrics as early warning signs of significant drivers of potential risks that exceed [Sample Client]'s risk tolerance statements. KRIs encompass internal and external risks which are mapped to key operational functions. KRIs are presented in a way that all employees clearly understand the significance and can respond accordingly.

At a minimum, [Sample Client]'s KRIs include the following:

- Details about the people, processes, technologies, facilities, and other corporate attributes most important to [Sample Client]'s continued operation and success
- Identified risks, threats, and vulnerabilities [Sample Client] faces, based on the likelihood of occurring, operational and financial impact to [Sample Client], and [Sample Client]'s ability to mitigate the event
- Ranking of business attributes based on criticality
- Ranking of risks, threats, and vulnerabilities in terms of their potential harm
- Linking of key business attributes to the most significant risks to identify the issues of greatest concern to [Sample Client]
- Metrics to identify when and how an identified risk becomes a serious threat to the critical attributes of [Sample Client]
- Ongoing process for reviewing KRIs and their metrics to identify changes that require management review and possible action
- Approval of KRIs by the chief compliance officer and chief risk officer

[Sample Client] regularly monitors and reviews KRIs to identify any situational changes that indicate a possible change in the business and risk/threat levels and to identify and initiate remedial action, as necessary.

Third-Party Service Provider Oversight

Compliance personnel monitor [Sample Client]'s third-party service providers through internal or outsourced audits annually. Audit results are reported to [Sample Client] management.

To limit the potential for statutory or regulatory violations and related consumer harm, [Sample Client] takes steps to ensure that its business arrangements with service providers do not present unwarranted risks to consumers.

3.3 Compliance Audit

3.3.1 Audit

Audit testing is performed less frequently and more formally than monitoring and is conducted by [Sample Client]'s Internal Audit Department or outside contracted party. To enable an independent audit process free from conflicts of interest, [Sample Client] establishes audit functions that are separate from operations tasks. Audit processes are separate from the activities being reviewed, and reporting structures reflect this segregation of audit functions and operations activities. The chief risk officer manages the audit program.

[Sample Client] recognizes the value of undergoing regular audits to measure, analyze, and progressively improve the effectiveness of its operations. The audit program reviews adherence to internal policies and procedures, and provides the board with determination of whether policies and procedures adopted to guide risk management are implemented and followed to provide the level of compliance and consumer protection established by the board. The audit program addresses compliance with all consumer protection-related laws and regulations.

The audit program's schedule and coverage are appropriate for [Sample Client]'s size, complexity, and risk profile. The Internal Audit Department maintains an annual schedule of audits planned for each department or functional area; however, audits may be amended or accelerated as needed to include new areas of regulatory or compliance risk. Planned testing may be eliminated or deferred at the request of senior management if resources reach capacity as areas of focus shift.

[Sample Client]'s senior management is responsible for the following:

- Promoting the concept of working collaboratively and cooperatively with auditors and examiners, with the goals of identifying operational weaknesses and faults, and remediating resulting issues to create overall improvement within the company
- Reviewing audit tracking reports and audit findings, and providing the necessary authority and direction required to remediate defects through the implementation of management action plans
- Escalating audit findings and management action plans with higher risk or impact levels to the appropriate committees or the board

Audit Objectives

The audit objectives are developed by the auditing entity and state the specific goals or hypotheses being tested. Management will request from the auditing entity a statement of

3.5 Vendor Management

[Sample Client] will abide by the requirements of its regulators by engaging in a rigorous analytical process to identify, measure, monitor, and establish controls to manage the risks associated with vendor relationships, and to avoid excessive risk-taking that may threaten [Sample Client]'s safety and soundness. Because vendor relationships are important in assessing the overall risk profile, the primary concern in reviewing relationships with vendors is to identify if [Sample Client] is assuming more risk than it can identify, monitor, manage, and control.

[Sample Client] recognizes multiple regulatory bodies that address and/or govern the management of vendor relationships.

Regulator	General Requirement
Consumer Financial Protection Bureau (CFPB)	The CFPB requires [Sample Client] to oversee business relationships with vendors through an appropriate risk management program. The depth and formality of the risk management program for service providers may vary depending upon the service being performed—its size, scope, complexity, importance and potential for consumer harm—and the performance of the service provider in carrying out its activities in compliance with federal consumer financial laws and regulations.
Federal Trade Commission (FTC)	The FTC provides regulations under the GLBA requiring that [Sample Client] has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information, including, but not limited to, the following: • Ensure the security and confidentiality of customer information • Protect against any anticipated threats or hazards to the security or integrity of such records • Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer
Federal Housing Finance Agency (FHFA)	When entering into vendor relationships, [Sample Client] can be exposed to financial, operational, legal, compliance, and reputational risk. The FHFA provides that effective risk