Table of Contents

TABLE OF CONTENTS **2**

SECTION 1 GENERAL **4**

1.1 STATEMENT OF PURPOSE 4
1.2 OBJECTIVE 4
1.3 STATE LAW AND AGENCY GUIDELINES 4

SECTION 2 SUMMARY **5**

2.1 COVERAGE 5

SECTION 3 REQUIREMENTS **6**

3.1 RISK MANAGEMENT GOVERNANCE 6
3.1.1 Board of Directors *6*
3.1.2 Risk Management Committee *6*
3.1.3 Individual Roles and Responsibilities *7*
3.2 IDENTIFYING RISKS 7
3.2.1 Credit Risk *8*
3.2.2 Market Risk *8*
3.2.3 Liquidity Risk *9*
3.2.4 Operational Risk *9*
3.2.5 Compliance and Legal Risk *9*
3.2.6 Reputation Risk *10*
3.2.7 Strategic Risk *10*
3.2.8 Inherent Risk *10*
3.3 DETERMINING RISK APPETITE 11
3.3.1 Overview of Risk Appetite *11*
3.3.2 Risk Appetite Review *11*
3.3.3 Communicating Risk Appetite *12*
3.3.4 Applying Risk Appetite *12*
3.3.5 Updating Risk Appetite *13*
3.4 MEASURING RISK 13
3.4.1 Quantitative Assessments *13*
3.4.2 Qualitative Assessments *13*
3.4.3 Assigning Significance *14*
3.5 ASSESSING RISK 14
3.5.1 Compliance Risk Assessment *15*
3.5.2 Operational Risk Assessment *17*
3.5.3 Marketing and Advertising Risk Assessment *19*
3.5.4 Consumer Complaints *24*
3.5.5 Credit Risk Assessment *26*
3.5.6 Hedging Risk Assessment *28*
3.5.7 Information Technology and Security Risk Assessment *29*
3.5.8 Third-Party Relationships *32*
3.5.9 Vendor Risk Assessment and Due Diligence *50*
3.5.10 Servicing Risk Assessment *51*
3.6 IMPLEMENTING A RISK MANAGEMENT STRATEGY 54
3.6.1 Risk Monitoring *54*
3.6.2 Internal Audit *54*
3.6.3 Stress Testing *54*
3.6.4 Risk Management Reporting *55*
3.6.5 Consequences for Insufficient Risk Management *55*

3.6.6 Maturing a Risk Management Program 56

SECTION 4 ORIGINATION COMPLIANCE 57

SECTION 5 SERVICING COMPLIANCE 58

SECTION 6 RECORD RETENTION 59

APPENDIX 1 DEFINITIONS 60

APPENDIX 2 EXHIBITS 63

FANNIE MAE TARGET DEFECT RATE TUTORIAL 63
POLICIES AND PROCEDURES CHECKLIST 64
CYBERSECURITY ASSESSMENT TOOL (FFIEC) 65

APPENDIX 3 BEST PRACTICES 69

INTERNATIONAL PROFESSIONAL PRACTICES FRAMEWORK 69
CORPORATE GOVERNANCE OF THE INTERNAL AUDIT FUNCTION 69
RATING AND REPORTING OF INTERNAL AUDIT ISSUES 70
COMMON INTERNAL AUDIT EXAMINATION ISSUES 71

APPENDIX 4 REFERENCE LIST 73

Section 2 Summary

This policy directs the risk assessment and management program of [Sample Client] and establishes minimum standards to maximize performance in overseeing the amount of acceptable risk in pursuit of strategic initiatives. It is the expectation of [Sample Client] that all risk management guidance be followed as directed in the identification, assessment, monitoring, and mitigation of risks to ensure compliance with regulatory requirements.

The standards set out in this policy represent minimum requirements for compliance with internal controls and assessment of risk management factors. These requirements are intended to prevent [Sample Client], its employees, and third-party vendors from violating federal regulations related to mortgage lending and consumer compliance.

2.1 Coverage

This policy addresses the implementation of risk management and consumer protection mechanisms as required and recommended by United States statutes and related federal regulations administered by the Consumer Financial Protection Bureau (CFPB) and other prudential regulators as identified by the CFPB including the Board of Governors of the Federal Reserve System (FRS), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), and the Office of the Comptroller of the Currency (OCC).

Section 3 Requirements

3.1 Risk Management Governance

3.1.1 Board of Directors

It is the responsibility of the board of directors, in cooperation with the risk management committee, to determine the allowable risks to the company. This determination is based on [Sample Client]'s ability to identify and understand applicable risks, measure the degree of exposure to risks, monitor the changing nature and exposure of certain risks, and develop processes and procedures to mitigate risks. The board of directors defines risk tolerances and ensures the review of periodic reporting to measure compliance with established risk limits. Reporting should include information regarding factors related to regulatory, technology, or personnel changes that may alter the risk exposure of [Sample Client].

3.1.2 Risk Management Committee

Reporting to the board of directors on a quarterly basis, the risk management committee (may also be known as the audit committee or executive committee) provides oversight of the financial reporting process, the audit process, the company's system of internal controls and compliance with laws and regulations. The risk management committee reviews risk and compliance issues, making recommendations for improvements. The risk management committee consists of, at minimum, the president, the chief executive officer, the chief financial officer, chief information security officer, chief operations officer, chief compliance officer, and/or chief risk officer. The focus of the committee is to review specific categories of risk as they relate to operations processes, information technology, and related security risks. The committee reviews the following:

- General or targeted risk assessment and performance indicators
- Internal audit reporting
- External audit results
- Capital market guidelines
- Underwriting guidelines and overlays
- Underwriting or pricing exceptions policies
- Other policies and procedures, as applicable

In addition to policy reviews, the risk management committee is responsible for ensuring procedures, programs, products, and practices align with company objectives using appropriate checks and balances. The risk management committee also monitors personnel and staffing to ensure employees are qualified, competent, and properly

3.5.1 Compliance Risk Assessment

The portion of the assessment related to compliance risk evaluates [Sample Client]'s effectiveness in following required regulations and guidelines in its daily operations. The results of this risk assessment are used as the basis for enhancing the compliance monitoring, testing, and audit program and ensuring the proper allocation of compliance resources.

3.5.1.1 Quality Control Monitoring

Establishing effective prefunding and post-closing quality control procedures allows [Sample Client] to assess trends that may increase the risk of repurchase or inability to sell its originated loans. Separating quality control responsibilities from the operation and production tasks enables the reporting of unbiased findings.

Pre-Closing Quality Control Reviews

The goal of pre-closing quality control reviews is to prevent errors by identifying issues and making corrections prior to the borrower signing closing documents, which may decrease the risk of repurchase. Pre-closing reviews are most effective when performed between underwriting approval and loan closing. Pre-closing quality control reporting includes sampling methodology, findings information, and trending details. Trends may warrant targeted post-closing quality control reviews to ensure the accurate and timely correction of errors.

3.5.1.2 Post-Closing Quality Control Reviews

In accordance with requirements of Fannie Mae, Freddie Mac, and the Department of HUD, [Sample Client] samples a minimum of 10% or uses a statistical sampling of originated loans during post-closing reviews. Common findings identified during audit are evaluated and corrective actions are issued for monitoring and improved compliance. Standardized review checklists ensure a thorough review and allow for the grouping of findings to create trending information.

3.5.1.3 Creating a Target Defect Rate

The board of directors and the management team establish a target defect rate as part of [Sample Client]'s risk management program. The target defect rate includes the maximum number of loans [Sample Client] is willing to originate that do not meet agency or investor guidelines. These loans may contain findings such as insufficient documentation, the inability to verify the documentation provided, or they may contain fraud or falsified documents.

3.5.3 Marketing and Advertising Risk Assessment

Advertising and marketing can provide consumers with valuable information regarding mortgage options, features, and costs that may be relevant to the decisions a consumer makes throughout the mortgage origination process. These advertising or marketing representations may be direct or implied in communication, but all statements must be perceived by consumers as reasonable. Reasonableness is evaluated based on sophistication and understanding of consumers and a claim may be susceptible to more than one reasonable interpretation. If one interpretation is misleading, then the advertisement is deceptive. In many circumstances, reasonable consumers do not read the entirety of an ad or are directed away from the importance of qualifying phrases, creating misunderstandings from the consumer's perspective.

Because interpretations may vary, [Sample Client] continually monitors commercial communications and consumer complaints for any possible misleading or misinterpreted claims. In addition, [Sample Client] monitors for any communications that are in blatant violation of required regulations. Commercial communications include, but are not limited to, the following:

- Any written or oral statement
- Illustrations, charts, or graphs
- Radio, television, magazine, or newspaper ads
- Infomercials or radio shows
- Direct mail
- Billboards or posters
- Internet, web pages, or e-mail communications
- In-person sales presentations

3.5.3.1 Unfair, Deceptive, and Abusive Acts and Practices

All marketing campaigns or advertisements to promote a loan originator, branch, loan product, or mortgage lending services must comply with applicable federal and state regulations.

3.5.3.2 Regulatory Requirements and Definitions

Section 5(a) of the FTC Act prohibits unfair or deceptive acts or practices in or affecting commerce.

Title X, Section 1036, of the Dodd-Frank Act prohibits unfair, deceptive, or abusive acts or practices in relation to consumer financial products and services.

may result in updates to risk management practices, [Sample Client] must maintain a complete inventory of its third-party relationships and periodically conduct risk assessments for each of the third-party relationships.

3.5.8.2 Third-party Relationship Life Cycle

Effective third-party risk management generally follows a continuous life cycle for third-party relationships. The following are the stages of the risk management life cycle.

It is important [Sample Client] involve staff with the requisite knowledge and skills in each stage of the risk management life cycle. [Sample Client] may involve experts across disciplines, such as compliance, risk, or technology, as well as legal counsel, and may engage external support when helpful to supplement the qualifications and technical expertise of in-house staff.

3.5.8.2.1 Planning

Effective planning allows [Sample Client] to evaluate and consider how to manage risks before entering into a third-party relationship. Depending on the degree of risk and complexity of the third-party relationship, [Sample Client] must consider the following factors, among others, in planning:

- Understanding the strategic purpose of the business arrangement and how the arrangement aligns with [Sample Client]'s overall strategic goals, objectives, risk appetite, risk profile, and broader corporate policies
- Identifying and assessing the benefits and the risks associated with the business arrangement and determining how to appropriately manage the identified risks
- Considering the nature of the business arrangement, such as volume of activity, use of subcontractor(s), technology needed, interaction with customers, and use of foreign-based third parties
- Evaluating the estimated costs, including estimated direct contractual costs and indirect costs expended to augment or alter [Sample Client] staffing, systems, processes, and technology
- Evaluating how the third-party relationship could affect [Sample Client]'s employees, including dual employees, and what transition steps are needed for [Sample Client] to manage the impacts when activities currently conducted internally are outsourced
- Assessing a potential third-party's impact on customers, including access to or use of those customers' information, third-party interaction with customers, potential for consumer harm, and handling of customer complaints and inquiries
- Understanding potential information security implications, including access to the [Sample Client]'s systems and to its confidential information

[Sample Client] may gain additional insight by evaluating processes for escalating, remediating, and holding management accountable for concerns identified during audits, internal compliance reviews, or other independent tests.

Information Security

The assessment of the third-party's information security program is a critical component of the due diligence process, [Sample Client] must include the following:

- The third-party approach to protecting the confidentiality, integrity, and availability of data
- Any gaps that present risk to [Sample Client] or its customers
- The extent to which the third-party applies controls to limit access to [Sample Client]'s data and transactions, such as multifactor authentication, end-to-end encryption, and secure source code management
- Whether the third-party keeps informed of, and has sufficient experience in identifying, assessing, and mitigating, known and emerging threats and vulnerabilities
- An assessment of the third-party's data, infrastructure, and application security programs, including the software development life cycle and results of vulnerability and penetration tests, as applicable

Due diligence can assist [Sample Client] in the evaluation of the third-party's implementation of effective and sustainable corrective actions to address any deficiencies discovered during testing.

Management of Information Systems

When technology is a major component of the third-party relationship, [Sample Client] must review both [Sample Client]'s and the third-party's information systems to identify gaps in service-level expectations, business process and management, and interoperability issues.

Additionally, [Sample Client] must include the of the third-party's processes for maintaining timely and accurate inventories of its technology and its contractor(s). [Sample Client] also benefits from understanding the third-party's measures for assessing the performance of its information systems.

Operational Resilience

The assessment of a third-party's operational resilience practices is critical to [Sample Client]'s evaluation of a third-party's ability to effectively operate through and recover from any disruption or incidents, both internal and external.

Appendix 2 Exhibits

Fannie Mae Target Defect Rate Tutorial

Fannie's Mae's Quality Control Self-Assessment Worksheet details procedures for creating an effective target defect rate.

Having a **target defect rate** is required for the top severity level (ineligible for delivery to Fannie Mae), and enables the lender to regularly evaluate and measure progress in meeting its loan quality standards. Lower severity levels must be defined by the lender as appropriate for its organization, and different target defect rates may be established for different severity levels (if applicable).

Calculating a defect rate is how you measure against your target defect rate. Some lenders use only a GROSS or a NET calculation when determining their monthly defect rate, while others use both. The GROSS defect rate is the defect rate based on the initial findings prior to any rebuttal activity. The NET defect rate is the defect rate based on the final findings after the rebuttal activity. **Understanding the root cause of the issues that were resolved during the rebuttal process may provide insight into how the defects can be prevented.**

If a loan has both a highest-severity level defect and a lower-severity level defect, only count the loan ONCE — in the highest-severity category — in a defect rate calculation.

The following are examples of calculating gross and net defect rates for a lender that has defined its defect categories as **significant** and **moderate**:

January Fundings: 1,000 loans | 10% QC Sample Selection: 100 loans

How to calculate a **gross** defect rate

This calculation should be done for your two most severe defect types (e.g., Significant and Moderate).

# of loans with a defect divided by **# of loans in the QC sample size**

example > # of loans with a significant defect: 5

5/100 = 5% gross significant defect rate

example > # of loans with a moderate defect: 10

10/100 = 10% gross moderate defect rate

How to calculate a **net** defect rate

(# of loans with a defect — # of corrected loans) divided by **# of loans in the QC sample size**

example > # of loans with a significant defect: 5 minus the # of resolved significant defects prior to the final QC report: 3

5 - 3/100 = 2% net significant defect rate

example > # of loans with a moderate defect: 10 minus the # of resolved moderate defects prior to the final QC report: 4

10 - 4/100 = 6% net moderate defect rate

Analysis and remediation – analyzing the defect

Once initial (gross) defects are cured, it is important to determine root causes, analyze issues, and reconcile the difference between your gross and net defects and action plan accordingly.

Analyze the cause between the gross and net defect rates. The goal is to identify and remediate the issues to narrow the gap between the gross and net defect rates.

How was the initial finding resolved prior to the distribution of the final QC report?

example > **Initial defect = insufficient income**

- Defect: All income documentation used to underwrite the file was not provided to QC for review.
- Resolution: During the rebuttal process, the additional income documentation missing from the QC file was provided.
- Action Plan: Implement processes/checks to ensure that all documentation used to underwrite the loan is in the file.

Cybersecurity Assessment Tool (FFIEC)

The assessment is completed through two parts, Inherent Risk Profile and Cybersecurity Maturity. For additional information, refer to the FFIEC Cybersecurity Assessment Tool User's Guide.

Inherent Risk Profile

Inherent risk levels are rated as follows:

- Least
- Minimal
- Moderate
- Significant or most

The Inherent Risk Profile includes a review of the following categories:

- Technologies and connection types: Higher inherent risk may exist depending on the complexity and maturity, connections, and nature of specific technology products or services used by [Sample Client], including the following:
  - Number of internet service providers (ISP) and third-party connections
  - Whether systems are hosted internally or outsourced
  - Number of unsecured connections
  - Use of wireless access
  - Volume of network device
  - End-of-life systems
  - Extent of cloud service
  - Use of personal devices
- Delivery channels: Higher inherent risk may exist depending on the nature of the specific products or services offered through the various delivery channels. Inherent risk increases as the variety and number of delivery channels increases and if services are available through online or mobile delivery channels.
- Online/mobile products and technology services: Higher inherent risk may exist through different products and technology services including an increased number of payment service types.
- Organizational characteristics: This category considers organizational characteristics, such as the following:
  - Mergers/acquisitions
  - Number of direct employees and cybersecurity contractors
  - Changes in security staffing
  - Number of users with privileged access