Table of Contents

trained. Lastly, the committee monitors system controls, including any risk models, internal/external audits, or quality assurance processes to confirm the effectiveness in managing applicable risks through adequate reporting.

3.1.3 Individual Roles and Responsibilities

The following individuals have direct involvement and responsibility for the risk management assessment process:

- The president and chief executive officer are primarily responsible for the management of strategic business decisions and technology risk.
- The chief financial officer is responsible for ensuring the accuracy of internal and external financial information, managing liquidity risks, and evaluating the risk of [Sample Client]'s investment portfolio.
- The chief information security officer is responsible for information technology risk management, including information technology security and data security services.
- The chief operations officer is responsible for all the following:
  - Working with appropriate parties to establish credit policies and standards
  - Developing reporting mechanisms and tools for monitoring compliance with lending policies
  - Evaluating the overall quality of the total loan portfolio
  - Identifying credit exposure trends
  - Evaluating the credit quality of individual loans
- The chief compliance officer or chief risk officer is responsible for all the following:
  - Maintenance of an appropriate compliance program
  - Compliance testing necessary to assess the adequacy of the program and to identify and correct compliance
  - Regulation monitoring and dissemination to the appropriate business units
  - Procedural, systematic, and regulatory compliance by business unit managers
  - Knowledge of regulations and guidelines among executives, managers, and staff
  - Maintenance of reference materials and compliance guides
- Internal auditors are responsible for the coordination of risk management and internal control processes, confirming that operating procedures, accounting controls, and security measures are commensurate with the expectations established by the board of directors.

3.6.6 Maturing a Risk Management Program

A mature risk management program requires board involvement, historical tracking, interpretive analysis, and corrective action. [Sample Client] also considers feedback from internal staff, regulatory agencies, and consumers to determine the best methods for improving marketing strategies, operational processes, and company culture.

The board and management prioritizes the annual risk assessment, demonstrating to all employees the importance of effective risk management. The board and management also communicates the results, recommendations, and resolutions with employees to quickly effect change and stress the importance of cohesion in adopting improvements. Lastly, results of the annual risk management assessment directly affect how resources are allocated. Risks can decrease with proper staffing and conversely, risks can increase with thin resources and lack of attention.

As [Sample Client]'s risk management program builds historical data and gains more discernable results, [Sample Client] can continue to expand its enterprise risk management qualitative and quantitative assessments across and into new business segments.

The following actions and attitudes ensure a progressive enterprise risk management strategy:

- Use risk management as a competitive advantage
- Involve the risk function in key decision-making
- Refine measurement and modeling of risks to facilitate a complete analysis and evaluation of risk scenarios
- Develop risk awareness across the organizational culture
- Focus on being proactive, rather than merely reactive
- Strive for continuous improvement

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