

# SECOND LINE TESTING

DEBORAH AUSTIN, CTCP  
FIDUCIARY COMPLIANCE  
DIRECTOR  
UNION BANK, N.A.



# BIOGRAPHY

DEBORAH AUSTIN

FIDUCIARY COMPLIANCE DIRECTOR

Deborah joined Union Bank in November 2008 responsible for managing fiduciary risk and compliance for Wealth Management and Institutional Services. These responsibilities include managing the fiduciary compliance program, business unit compliance risk assessments, third party compliance risk assessments, personal security transactions trading activities, conflicts of interest, managing the fiduciary compliance program and integration projects. Deborah has over 32 years in banking.

Prior to Union Bank, Deborah was the Fiduciary Compliance Manager for PNC and the Chief Compliance Officer for PNC Building Investment Trust. Moving to PNC from Glenmede Trust Company where Deborah served in fiduciary audit and risk management, building out the fiduciary risk program.

Deborah is past president and board member of FIRMA. She is currently the chair of the Fiduciary Compliance and Risk Roundtable and FIRMA Second Line of Defense Peer Group.

# AGENDA

I. TESTING PROGRAM

II. TESTING INVENTORY

III. RISK ASSESSMENT

IV. TESTING SCHEDULE

V. TESTING EXECUTION

VI. INHERENT RISK RATING DEFINITIONS

VII. OTHER TESTING, MONITORING, REVIEWS

VIII. WRAP UP DISCUSSION

DISCLAIMER: This presentation is provided for informational and educational purposes only. The opinions and views expressed represent thoughts of the author and do not necessarily reflect those of Union Bank.

# I. TESTING PROGRAM



- Drivers:
  - FRB SR 08-8
  - 12 CFR part 30, appendix D
- Components
  - General Overview
    - Purpose, scope, applicability
  - Policy Statement
    - Risk assessment, planning, execution, disputes, issue ratings, communications
  - Roles and responsibilities
    - Define who does what

## II. TESTING INVENTORY

### □ Where to start?

- Family, Friends, Neighbors
- Regulator
  - Handbooks
  - Manuals
- Third Party
  - Archer
  - Consultants
  - StateScape

# III. RISK ASSESSMENT

- COSO (Committee of Sponsoring Organization of the Treadway Commission)
  - Compliance Risk Assessment Standards
  - Phases
    - Planning
    - Execution
    - Assessment frequency
    - Assessment of inherent risk and ratings
    - Evaluations of effectiveness of internal controls and ratings
    - Determination of residual risk and risk ratings

### III. RISK ASSESSMENT cont.

- Risk assessments ultimately should document significant risks to the business, results which guide 2<sup>nd</sup> line to determine what to test, the scope and objective. The results of the assessment should be used to focus on areas of high, moderate high risk and sets the priorities for testing.
- Becomes the topic universe or matrix, a list of the regulations, laws, rules, subjects, and processes from which there grows the the testing schedule.
- The topics through completion of the risk assessment are assigned ratings. The rating then determines the frequency.

### III. RISK ASSESSMENT cont.

Inherent or Residual Risk	Testing Frequency
High or Moderate High Risk	Annual
Moderate or Low Moderate Risk	12 -18 months
Low Risk	18 - 38 months

Frequency should be adjusted based on the following:

- Other testing, monitoring, exams results, changes in a regulation or law
- Bankwide elevation in risk
- Specific area of regulatory scrutiny or heightened expectations
- New products and/or services

## IV. TESTING SCHEDULE

- Risk based
- Drafted annually
- Re-assessed quarterly
- Provides a formal plan
- Flexible
- Reviewed with First Line
- Approved by Second Line Management

# V. TESTING EXECUTION

□ Planning

□ Communication

□ Scope

□ Issues

□ Reporting Results

# VI. Inherent Risk Rating Definitions

Risk Category	Definition
Higher Risk	Exists when there is significant risk of non-compliance and the impact of non-compliance could be severe
Moderate Risk	Exists when there is some risk of non-compliance and potential impact of non-compliance is moderate
Lower Risk	Exists when there is lower risk of non-compliance and potential impact of non-compliance is low

## VII. Other Testing and Monitoring

- First Line (AKA 1.5)
- Second Line Monitoring
- Internal Audit
- Regulatory Examinations

# VIII. Wrap Up Discussion