COMPLIANCE BEYOND THE BASICS

FIRMA Annual Fiduciary Management Conference

May 3, 2023

BIOGRAPHY

David S. Villwock

JPMorgan Chase Bank, N.A.

Compliance Managing Director
US Private Bank Compliance
Head of Firmwide Fiduciary Compliance

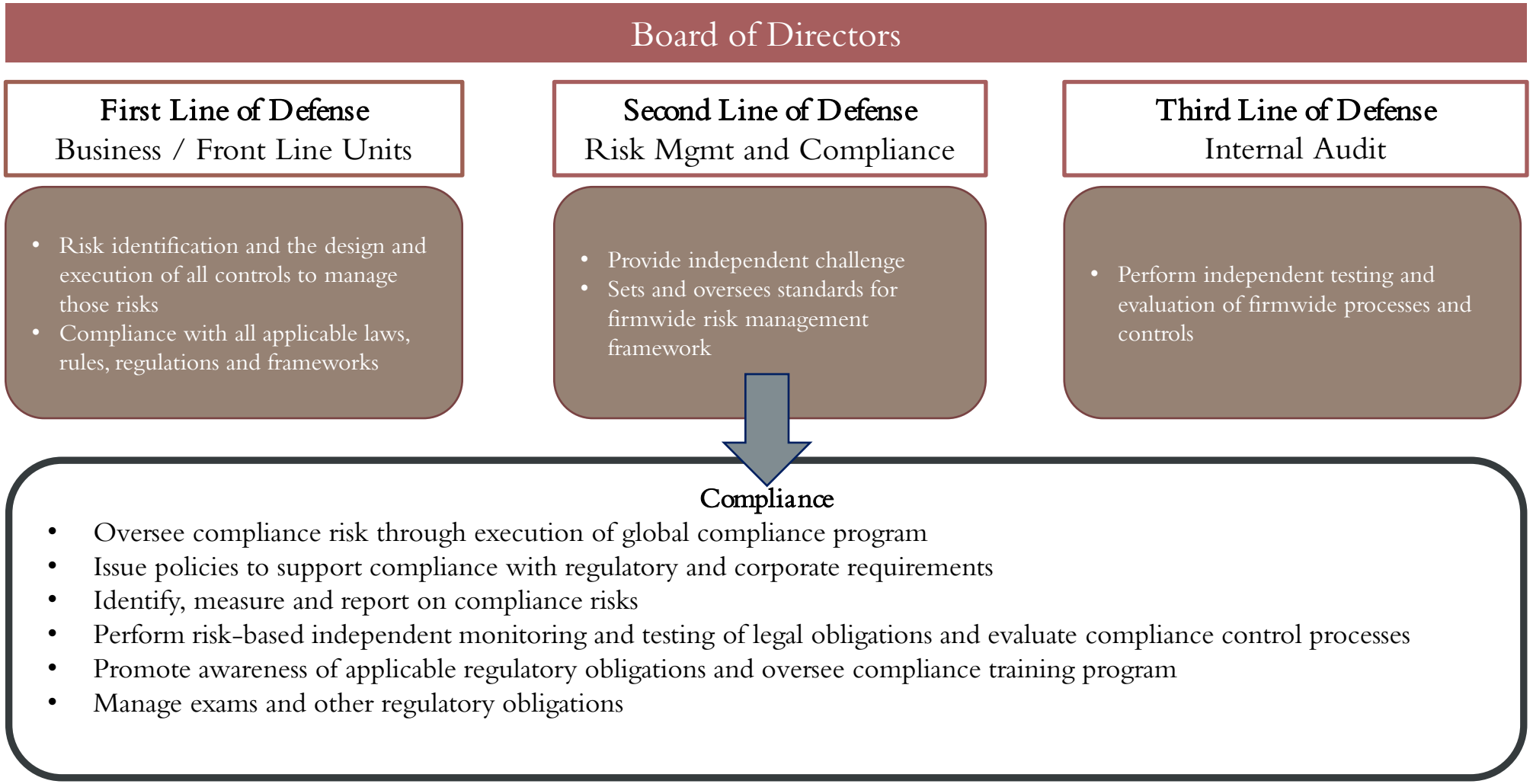
Columbus, OH
Email: david.s.villwock@jpmorgan.com
Phone: (614) 248-0952

David Villwock is the Head of JP Morgan's US Private Bank Compliance and serves as the Head of JP Morgan Firmwide Fiduciary Compliance where he has responsibility for JP Morgan's compliance infrastructure for obligations under Part 9 and ERISA for all lines of business. He also serves as the firm's Senior Compliance Officer under the Qualified Professional Asset Manager (QPAM) exemption.

He joined JP Morgan in 1999 managing large scale regulatory projects focused on fiduciary account system conversions, investment performance system conversions and related operations consolidations. He joined the Compliance team in 2006. Before coming to JP Morgan, Mr. Villwock operated a law practice focused on trust and estate and employment law. He has a BA from Otterbein College, a JD from the DePaul University College of Law and an MBA from The Ohio State University.

He is a member of the Ohio Bar and has earned the Certified Fiduciary & Investment Risk Specialist (CFIRS) designation from Cannon Financial Institute.

THREE LINES OF DEFENSE



ELEMENTS OF AN EFFECTIVE COMPLIANCE PROGRAM

Govern

Policies

Standards

Training

Identify

Risk Lexicons

Risk Subdivisions

Risks assigned to areas of the firm

Measure

Risk Assessment

Challenge of 1LOD

Drivers of Risk

Magnitude and Likelihood

Monitor and Test

Ongoing review

Periodic deep dive

Test outcomes and effectiveness of controls

Manage

Issue Management

Issue Validation

Metric Reviews

Report

Dashboard

Committee Updates

Escalation Criteria

Committee participation

BEYOND THE BASICS – FOCUS AREAS

Govern

- Policies
- Standards
- Training

Identify

- Risk Lexicons
- Risk Subdivisions
- Risks assigned to areas of the firm

Measure

- Risk Assessment
- Challenge of 1LOD
- Drivers of Risk
- Magnitude and Likelihood

Monitor and Test

- Ongoing review
- Periodic deep dive
- Test outcomes and effectiveness of controls

Manage

- Issue Management
- Issue Validation
- Metric Reviews

Report

- Dashboard
- Committee Updates
- Escalation Criteria
- Committee participation

EXAMPLES

- 12 CFR 9.6 (a-c) – Review of fiduciary accounts (Pre, Initial, Annual)
- 12 CFR 9.10(b)(1) – Fiduciary funds awaiting investment or distribution, Self-Deposits
- Reg R Trust and Fiduciary Exemption – Chiefly Compensated Test

12 CFR 9.6 (a-c) – REVIEW OF FIDUCIARY ACCOUNTS (PRE, INITIAL, ANNUAL)

(a) Pre-acceptance review. Before accepting a fiduciary account, a national bank shall review the prospective account to determine whether it can properly administer the account.

(b) Initial post-acceptance review. Upon the acceptance of a fiduciary account for which a national bank has investment discretion, the bank shall conduct a prompt review of all assets of the account to evaluate whether they are appropriate for the account.

(c) Annual review. At least once during every calendar year, a bank shall conduct a review of all assets of each fiduciary account for which the bank has investment discretion to evaluate whether they are appropriate, individually and collectively, for the account.

- See also FDIC Trust Examination Manual Section 1 – Management, F – Account Review Program

12 CFR 9.10 (b)(1) – FIDUCIARY FUNDS AWAITING INVESTMENT OR DISTRIBUTION - SELF DEPOSITS

b) Self-deposits -

(1) In general. A national bank may deposit funds of a fiduciary account that are awaiting investment or distribution in the commercial, savings, or another department of the bank, unless prohibited by applicable law. To the extent that the funds are not insured by the Federal Deposit Insurance Corporation, the bank shall set aside collateral as security, under the control of appropriate fiduciary officers and employees, in accordance with paragraph (b)(2) of this section. The market value of the collateral set aside must at all times equal or exceed the amount of the uninsured fiduciary funds.

- See also FDIC Trust Examination Manual Section 8 – Compliance/Conflicts of Interest, Self-Dealing and Contingent Liabilities, E.3. Use of Own-Bank or Affiliate Bank Deposits

REGULATION R: EXCEPTION FOR BANKS FROM THE DEFINITION OF A BROKER – TRUST AND FIDUCIARY EXEMPTION

§ 247.722 Exemption allowing banks to calculate trust and fiduciary compensation on a bank-wide basis.

(a) General. A bank is exempt from meeting the "chiefly compensated" condition … to the extent that it effects transactions in securities for any account in a trustee or fiduciary capacity … if:

1. The bank meets the other conditions for the exception from the definition of the term "broker"… including the advertising restrictions … and
2. The aggregate relationship-total compensation percentage for the bank's trust and fiduciary business is at least 70 percent.

- *17 CFR 247.722*
- *See also FDIC Trust Examination Manual, Section 10 F(a)(1) and Appendix D – Securities Law; (2) Bank as Broker*

GOVERN

Rules

- In order to establish a compliance framework, first identify and create the rules which will govern your activities. These come from:
  - Laws regulations and other jurisdictional rules
  - Corporate standards
  - Regulatory experiences
  - Guidance on proper risk controls

Artifacts

- Policies and Manuals
- Standards
- Rules of the Road
- Analysis of legal requirements
- Training Guides

Ongoing Maintenance and Training

- Regulatory Change Management processes
- Training Needs Analysis and Plan

GOVERNANCE DOCUMENTS

Policies

- A document that sets forth principles and foundational concepts through high-level statements of direction and scope and aligns the firm to achieve its objectives
- Policies are appropriate when there is a legal obligation or regulatory requirement for a policy, or if the firm needs to establish high-level principles.

Standards

- A document that states mandatory requirement and/or establishes minimum requirements to be executed to satisfy a firm policy or other criteria.
- If a standard supports a policy the standard must not conflict with, be less restrictive, or expand on the policy.

POLICIES AND STANDARDS

Content must be:

- Actionable
- Measurable
- Enforceable

Documents must be:

- Reviewed periodically or upon changes of underlying rules, business activities, regulatory interpretations
- Consistent and integrate with other policies and standards
- Well-socialized both from input and from a communication perspective
- Linked to legal and regulatory obligations

Best practices:

- Identify clearly which parts of the company are subject to the policy as well as the owner/contact for additional questions
- List and link to related policies and other documents
- Use present tense and Active voice
- Avoid jargon and abbreviations/acronyms unless including will save significant space and then define on first instance
- Do not paraphrase regulations, refer to them clearly and link where necessary
- Use absolutes (e.g., all, any) intentionally and sparingly. Be clear when using "must" or "shall" vs. "may" statements
- Use inclusive language
- Identify changes from previous version clearly

TRAINING

Governance:

- Training Needs Analysis (leverage Risk Assessment results, date of last training, changes in industry to determine needs)
- Content/Approach (Live/In Person, Virtual Live, Computer aided etc., Bulletin)
- Audience Assignment – Frequency and New Joiners
- Mandatory vs. Suggested
- Tracking/Completion
- Consequences for failing to complete including repeat offenders

Best practices:

- User specific examples from their area of coverage
- Completion tests help to demonstrate understanding of the minimum
- Calendar to track regulatory obligations and completion of training agenda and reduce training fatigue/time commitment from audience
- Use of vendors or centralized utility vs Compliance team.

MONITOR AND TEST

M&T Plan and Execution

- Utilize CRA results and other feedback to develop a plan and communicate to stakeholders in advance
- M&T should be well documented, auditable, objective, tied to the CRA results, sustainable
- Consider pros and cons of dedicated testing staff vs. using advisory Compliance personnel

Points to Consider

- Monitoring is a repeatable review of risk that operate best when automated, have high sample rates and identify deviations from controls over time
- Testing is a deeper review and is more resource intensive
- Manage overlap from other auditors or regulators in the same area

Coverage

- Establish a frequency guide tied to the results of the CRA
  - Low RR items can be grouped into less frequent tests
  - High RR items covered each year
- Identify appropriate exceptions to the coverage model (e.g., issue already documented in area to be examined)

TESTING

- Independent risk-based, point-in-time evaluation of the control design adequacy and execution effectiveness to mitigate compliance risks.
- Accomplished through a comparison of actual processes against expected practices identified through policies, standards, procedures, laws, rules and regulations.
- Testing also evaluates whether processes, risks and controls are appropriately documented by the 1LOD.

TESTING DOCUMENTATION

- Test background and scope including:
  - identification of specific risk and area to be tested,
  - policies and procedures to be reviewed,
  - results of prior exams and audits,
  - open or recently closed issues
- Announcement Memo and test plan
  - Scope of test
  - Communication method/frequency of updates
  - Start and estimated Completion Time
- Test Scripts
  - Description of test including objective and steps
  - Sampling methodology and approach including a description of the population being tested
  - Description and source of supporting documentation
  - Copies of supporting documentation and examples
  - Details of observations/exceptions and issues noted
  - Review of control design and documentation
- Evaluation of Results
  - Investigate Root Cause of any exceptions noted
  - Examine prevalence, materiality, tolerance, root cause, existence of subjectivity to process to determine if it rises to an issue
  - Document rationale for disposition of all exceptions and communicate to 1LOD
- Final Report and assignment of issues
  - Executive Summary
  - Scope
  - Detailed Issues and Management Action plans
  - Confirm distribution list.
- Closure of Issue validation
  - Did they close the control issue?
  - Is the control sustainable?
  - Manager review to ensure consistency and completeness of documentation

MONITORING

- Ongoing evaluation and identification of compliance risk exposure and control effectiveness in business processes.
- Monitoring maximizes coverage of risk evaluation by reviewing processes, risks and specific control performance on a regular basis.
- Monitoring activities are repeatable and happen more frequently than testing items (generally annually or more frequently)

MONITORING DOCUMENTATION

- Identify Activity in a tracking/plan tool
  - Name and Objective
  - Scope
  - Frequency
  - Performer of activity and Review Team
  - Steps
  - Tag relevant risks from the risk assessment
  - Data source and description of the population used and how obtained
- Identify results
  - Sample size and methodology
  - Time period in scope
  - Any changes to procedures with rationale
  - Results and disposition of any exceptions
  - Identify issues and get agreement to action plans and ownership from 1LOD
- Consider applicability of Machine Learning and Artificial Intelligence strategies to assist with increasing coverage and efficiency of monitoring activities.

MANAGE

Issues identified by Compliance

- The firm should have an issue resolution process that includes issues identified by all lines of defense, regulators and others.
- Compliance should leverage that process but maintain independence to generate issues without being vetoed or diluted by the issue management process owners.

Source of Compliance Issues

- Day-to-day Compliance Advisory Coverage
- Monitoring, including investment surveillance
- Testing
- Regulator recommendations or other commentary
- Response to high RR noted in CRA

Tracking and Closure

- 1LOD should follow a well documented issue tracking and closure process
- Compliance will need to challenge:
  - Effectiveness of proposed plans
  - Timeliness of plans
  - Completeness of action taken
- Compliance retesting and challenge

ISSUE MANAGEMENT

- Issue Creation

  Name, Description, how identified, date identified, owner, target date (including time for proving sustainability)

  Issue Root Cause Analysis

  Issue Severity Rating (consider business and economic, regulatory, reputational, client, legal, and market impacts of the issue)

  Record issue in firm's issue management system.

- Action Plan Development

  Issue Remediation (promptly to mitigate risk and potential non-compliance)

  Control Action Plan (s)

    Owner and Target Date

    Watch out for Plan for Plans

    Consider compensating controls for long dated plans

ISSUE MANAGEMENT

- Issue Change Management

  Approvals for changes to severity

  Approvals for changes to target date

  What's wrong with going red?

- 1LOD Issue Validation

  Issue Owner signs off as complete

  Independent testing of control to confirm work is complete and accomplished goal

  Consider standalone process with Independent testing for significant regulator identified issues.

- Issue Completion

- Compliance Issue Validation

  For appropriate severity issues, Compliance should include issue validation as part of a test plan relatively soon after the 1LOD closes a Compliance identified issue.

REPORT

Dashboard

- Compliance must develop an effective process of communicating CRA results, M&T results, issues, and ongoing advisory items
- Technology and dashboard development are effective means to communicate

Governance

- Compliance must have a seat at significant committees
- Their role is to:
  - Challenge the 1LOD on actions, decisions, new business, exceptions
  - Report on the effectiveness of the Compliance program
- Compliance must have the ability to restrict activity where warranted (i.e., have stature in the Committee).

Board of Directors

- The BOD has the ultimate responsibility for the control infrastructure.
- Compliance should help ensure that the board is properly informed, governance structure makes sense and is organized to provide transparency and allow for resolution of issues.
- Compliance can and should ensure that matters requiring BOD attention are escalated.

APPENDIX

Compliance Basics - Risk Assessment Slides

IDENTIFY

Compliance Risk Causes

- Violations of laws and regulations
- Nonconformance with prescribed practices, internal policies or ethical standards
- Which can incur:
  - increased legal and reputation risks
  - enforcement actions
  - customer reimbursements
  - diminished reputation
  - harm to bank customers
  - limited business opportunities
  - lessened expansion potential

Risk Identification

- Create a process for categorizing and identifying risk
- Needs to be a continual process
- Should occur at the transaction, portfolio and enterprise levels
- Board and Management should identify correlations and interdependencies across lines of business that may amplify exposures.

Artifacts

- Risk Lexicons
- Risk Hierarchy
- Risk Assignment to business units and processes
- Material Risk Inventory
- Risk Appetite

MEASURE

Compliance Risk Assessment (CRA)

- Detailed analysis of the level of compliance risk inherent in a process
- The CRA will result in a calculated level of residual risk useful in assigning resources to minimize control gaps on a risk-adjusted priority basis

Probability and Severity

- Risks sourced from the lexicon and hierarchy
- The CRA breaks down the organization into useful units for assessment of the risk
- Risks are evaluated as to the likelihood of occurrence and the magnitude of risk

Inherent Risk

- Risk of loss when no controls are applied
- Consider changes in:
  - New rules or laws
  - Industry
  - Regulatory focus
  - Recent areas of concern from other firms.

Control Effectiveness

- Assessors identify the quality of controls in place
- Reference a variety of information including
  - 1LOD analysis of controls
  - Issues
  - Complaints
  - Regulatory findings
  - 2LOD Analysis
  - Audit findings
  - Similar control issues from other parts of the firm or industry

Residual Risk

- Risk leftover when applying the effect of controls
- Calculated using the IR and CE scores
- By reviewing areas of higher residual risk, Compliance can prioritize resources:
  - 2LOD Testing
  - Technology enhancements
  - Process enhancements