The Compliance Testing Program

Utah Bankers Association

2020 Virtual Fall Compliance Conference

October 28, 2020

Presenter: Lourdes Johnson, CRCM, CAMS

"What Does a Comprehensive/Robust Compliance Testing Program Look Like?"

- Linkages to the Compliance Management System
- Elements of an Effective Compliance Testing Program
- Regulator Expectations & ***Industry Best Practices***

The Compliance Testing Program

- In today's regulatory environment where the bar is set high by banks and regulatory agencies for a bank's Compliance Management System (CMS) to be comprehensive and robust, one of the ***key*** elements of a viable CMS is an effective and efficient Compliance Testing Program.
- Effective compliance testing programs identify non-compliance with laws, regulations, and bank policies at the earliest stage possible.
  - **Stage 1- First Line of Defense: Business units conduct self-monitoring and testing**
  - **Stage 2- Second Line of Defense: Compliance Risk Management conducts monitoring and testing**
  - **Stage 3- Third Line of Defense- Internal and/or external Audit conduct independent testing ("audits")**

Compliance Management System

Compliance Management System
Monitoring/Testing/Audit

1st Line

- Self-Testing (i.e. Quality Control Monitoring Reviews)
- Risk Control Self-Assessment (RCSA)

2nd Line

- Quality Assurance Monitoring Reviews (i.e. "Test the Tester")
- Compliance Testing

3rd Line

- Independent Audit (Internal / External)

Elements of an Effective Compliance Testing Program

1. Build & Maintain a Requirements Library
2. Develop the Compliance Test Plan
3. Establish Testing Methodology
4. Link the Test Plan to Critical Elements of the CMS
5. Create an Effective Communication Plan for the Entire Test Cycle

Elements of an Effective Compliance Testing Program

6. Execute the Compliance Test
   - Conduct the Test
   - Communicate & Report Results
   - Record and Track Issues
   - Validate Issue Remediation and Sustainability
7. Conduct a Trend Analysis

Step 1- Build & Maintain a Requirements Library

The Requirements Library:

- identifies all laws and regulations ("requirements") that are applicable to the bank, to include new and changing requirements
- maps the requirements to each applicable business unit
- **is built in collaboration with the 1st and 2nd line of defense subject matter experts (SMEs) - (Legal Services is consulted as needed)**
- **ranks the requirements following a risk-based approach**
- **(Note: For mature CMS Programs, the Library aligns with the Risk Control Self-Assessment (RCSA), and is retained in the Governance/Risk/Compliance (GRC) tool)**

Step 2- Develop the Compliance Test Plan

The Compliance Test Plan ("Test Plan"):

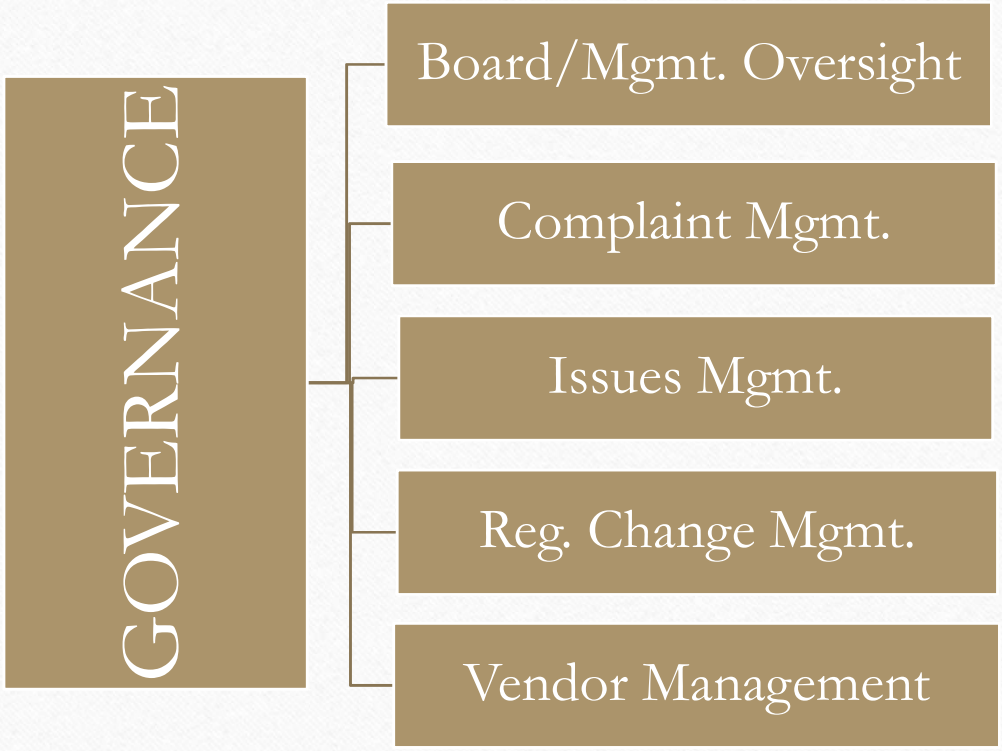
- utilizes the Requirements Library as its foundation
- follows a risk-based approach and is informed by key elements and data from the CMS to include: policies, procedures, training, issues, complaints; and results of the Compliance Risk Assessment, RCSA, compliance tests, audits, and regulatory examinations
- follows a schedule, generally an annual schedule executed in increments (i.e. quarterly)
- is approved by the applicable governing committee (i.e. Compliance Risk Management Committee)
- is communicated to 1st and 2nd line partners following the Communication Plan
- provides reporting to the governing committee on a regular cadence (i.e. monthly, quarterly, etc.)- reporting includes test results and non-adherence to schedule

Step 3- Establish Testing Methodology

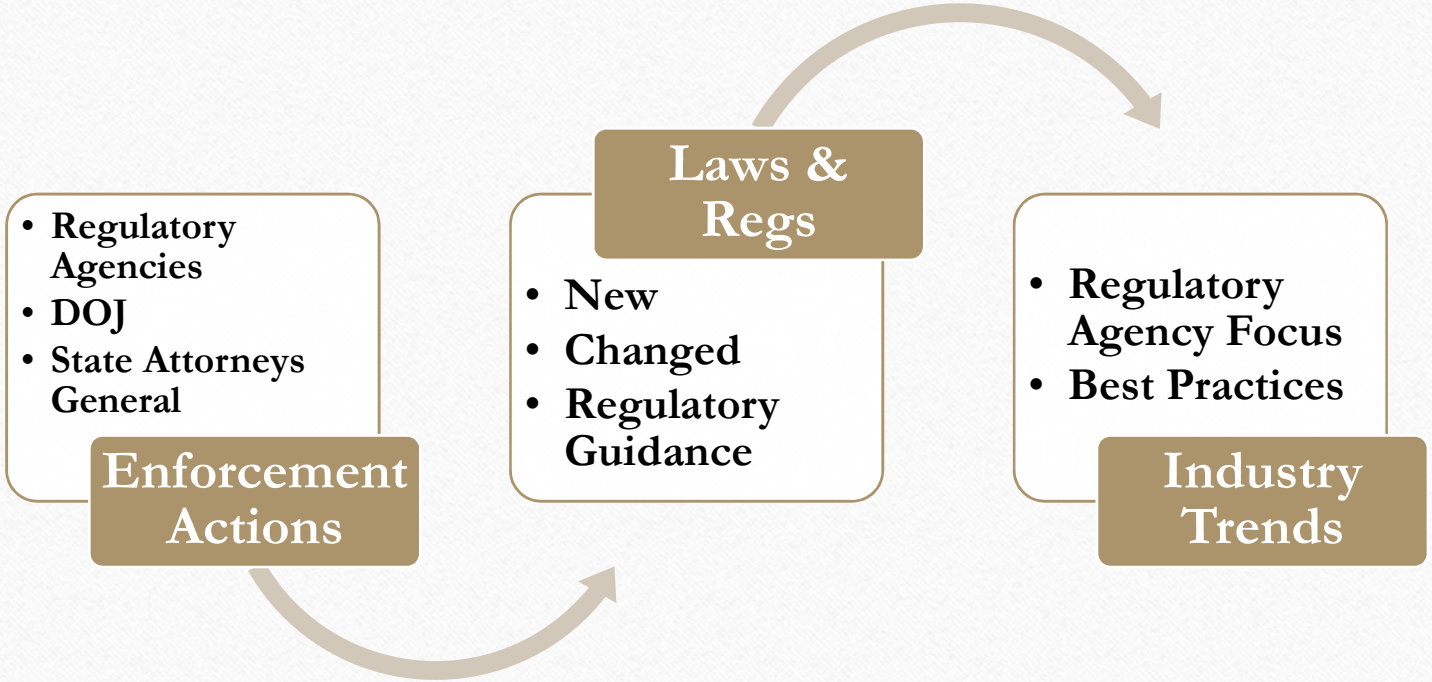
The Testing Methodology:

- establishes the requirements, controls and business units to be tested
- utilizes comprehensive regulatory checklists
- includes transaction testing
- defines the following:
  - testing approach (purpose/scope/objectives/test period)
  - sampling methodology
  - process for managing identified issues (reporting, escalation, tracking, and validation of remediation plans for closure, completeness and sustainability (creating a "closed-loop process")

Step 4- “Example Link to the CMS”



Step 4- "Example Link to CMS" Regulatory Change Management



Step 5- Create an Effective Communication Plan for the Entire Test Cycle

The Communication Plan:

- is in writing and provides ample advance notice to area being tested ("Auditee")
- provides information regarding: the purpose/scope/objectives/test period/testing methodology
- describes the ongoing communication process to include: recurring meetings, status updates and the exit meeting
- describes process for reporting test results to bank management and the applicable governing committee

Step 6- Execute the Compliance Test

The Compliance Test:

- is conducted (started/executed/finalized) in accordance with the testing methodology and communication plan
- documents results in writing and retains supporting artifacts
- provides results to the Auditee for review and response
  - **for identified issues, the Auditee identifies the "root-cause" and establishes a remediation plan which is reviewed and approved by the 2nd line of defense**
  - **identified issues are recorded in the GRC tool for remediation. The remediation plan is validated by the 2nd line of defense for completeness and sustainability**
- results are reported to bank management and the applicable governance committee

Step 7- Conduct Trend Analysis

Conducting a trend analysis provides:

- a view of the health of compliance of the bank (test period over test period)
- a view by business unit of where non-compliance to requirements exists
- a holistic view for the bank of where non-compliance to requirements exists
- an understanding of gap frequency (i.e. newly identified gap vs recurring gap)
- data which helps inform the test plan on a go-forward basis

Conclusion

- ***Regulators expect that a bank's Compliance Management System (which includes the testing program) will be commensurate with the size and complexity of the bank and the products and services offered by the bank.***
  - "Robust compliance monitoring and testing play a key role in identifying weaknesses in existing compliance risk management controls and are, therefore, critical components of an effective firm-wide compliance risk management program."*****
  - "Compliance testing is necessary to validate that key assumptions, data sources, and procedures utilized in measuring and monitoring compliance risk can be relied upon on an ongoing basis and, in the case of transaction testing, that controls are working as intended. The testing of controls and remediation of deficiencies identified as a result of testing activities are essential to maintaining an effective internal control framework."*****
    - *****Source: Federal Reserve Bank publication: **SR 08-8 / CA 08-11**

Questions & Answers

Thank you for your time and participation!