



SOLIDBUILT BANK

# FIDUCIARY COMPLIANCE

Fiduciary Compliance Testing  
Group

v.3.5 May 2023



## Table of Contents

PURPOSE	2
POLICY STATEMENT	2
ROLES AND RESPONSIBILITIES	2
TESTING SCOPE AND FREQUENCY	4
TESTING SCHEDULE	4
AMENDMENTS TO THE ANNUAL TESTING SCHEDULE	5
TESTING EXECUTION	6
TESTING CYCLE	6
<i>Planning</i>	6
<i>Fieldwork</i>	7
<i>Reporting</i>	10
QUALITY CONTROL	12

# SOLIDBUILT BANK

## FIDUCIARY COMPLIANCE TESTING PROGRAM

### PURPOSE

To independently test compliance risks and controls that the 1<sup>st</sup> line business unit is responsible for and owns the risks. Fiduciary Compliance Testing is a point in time evaluation of processes or controls and adherence to Federal and State regulations.

### POLICY STATEMENT

The Fiduciary Compliance Testing Program (The Program) describes the testing framework for the SolidBuilt Bank's Compliance Testing Unit. The Board of Directors and senior management of SolidBuilt Bank recognize the importance of an effective testing program that identifies risks in a timely and proactive manner and manages risks ensuring continued compliance with fiduciary related regulatory requirements. It is the mission of fiduciary compliance testing to implement and maintain a strong compliance testing program that aligns with the bank's vision.

Per the Board of Governors of the Federal Reserve System's SR 08-8 Letter, compliance testing is a critical component of sound compliance risk management and serves as the basis for evaluating the effectiveness of the Bank's control environment, compliance and operating effectiveness with respect to regulations and other requirements.

The Testing Unit is responsible for developing, implementing and maintaining effective viable testing procedures that contain elements described within this program. The Testing Unit has the authority to access all Bank records and communicate directly with Bank employees.

### ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITIES
Testers and Testing Leads	<ul style="list-style-type: none"><li>▪ Work with compliance officers, line of business and legal if necessary to assess testing priorities.</li><li>▪ Determine the testing inventory.</li><li>▪ Create the testing schedule.</li><li>▪ Work with testing management to ensure coverage of regulations applicable to the business unit.</li><li>▪ Determining an appropriate approach for the execution of assigned testing.</li></ul>

	<ul style="list-style-type: none"> <li>▪ Testing leads will direct staff on assignment.</li> <li>▪ Review the schedule with monitoring activity heads, internal audit and applicable business units and make schedule adjustments as necessary.</li> <li>▪ Escalation of issues or matters impacting the progress of the test</li> <li>▪ Compile the work papers for manager review and approval</li> <li>▪ Obtain approval of the testing schedule from the head of testing.</li> </ul>
Testing Head	<ul style="list-style-type: none"> <li>▪ Implements a governance framework for compliance testing.</li> <li>▪ Assures that the testing team has the authority, independence, requisite, expertise and resources.</li> <li>▪ Determine that the testing universe is accurate and complete.</li> <li>▪ Determine the level of resources required to implement the testing schedule.</li> <li>▪ Identify opportunities for joint testing.</li> <li>▪ Approving the final testing schedule and any changes and that changes are sufficiently justified.</li> <li>▪ Prepare the final testing schedule for submission to risk &amp; compliance management.</li> <li>▪ Publication and distribution of testing schedule.</li> <li>▪ Provide periodic updates to applicable committees and compliance executive management.</li> </ul>
Chief Compliance Officer	Responsible for reviewing and approving the Compliance Testing Universe and schedule.
Business Unit	<p>The business unit is responsible for ensuring that fiduciary compliance risk management as part of each employee's daily job function. Business units are the first line of defense, and their procedures training and other controls are critical to the prevention detection and correction of fiduciary compliance related concerns.</p> <p>Business unit fiduciary compliance related responsibilities include:</p> <ul style="list-style-type: none"> <li>▪ Selecting and implementing risk management strategies</li> <li>▪ Identifying and measuring risk exposures</li> <li>▪ Assisting in the creation and maintenance of appropriate policies and associated procedures</li> <li>▪ Incorporating free, Sherry compliance elements into the business units strategies and significant new initiatives by implementing appropriate internal controls</li> <li>▪ Establishing appropriate controls and employing methods for assessing the effectiveness of those controls</li> </ul>

	<ul style="list-style-type: none"> <li>▪ Employing staff with requisite experience and knowledge training and management skills</li> </ul>
--	--

## TESTING SCOPE AND FREQUENCY

The fiduciary testing program covers compliance with federal and state laws, regulations and supervisory guidance. The scope of areas to be reviewed will follow a risk based approach that will consider the level of inherent and reschedule risk adequacy of controls the business unit, compliance risk assessment, new or evolving regulatory expectations, internal audit, examinations, and regulatory examinations.

Compliance Risk Assessments are a core component of an overall risk management program. It serves as the main driver for determining the regulations and key processes that will be subject to testing and ultimately defines the scope. Testing frequency is risk-based on the inherent risk rating of the regulations and processes as identified in the Compliance Risk Assessment. Testing frequency is further defined by changes to regulations, process and product changes in the 1<sup>st</sup> line business unit, past findings and issues, control effectiveness and the regulatory environment.

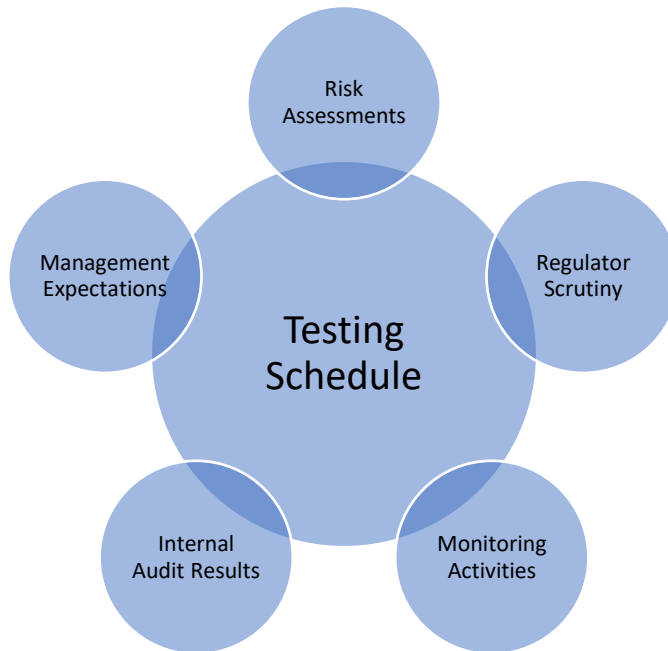
### Testing Frequency

Risk Rating	Frequency
High	12 months
Moderate	24 months
Low	48 months

Testing frequency can be influenced by other testing, monitoring or internal audit results. Other instances for changing the frequency or target testing is regulatory scrutiny, new products/services, client complaints and time since the prior test. Frequency and changes to frequency must be documented, justified and approved by the Head of the Testing Unit.

## TESTING SCHEDULE

The Testing Schedule is based on the risk rating of the regulation, processes and products. The risk rating of which is produced from the annual risk assessment as well as other elements used to determine the frequency.



The testing schedule is to be reviewed with the business units effected prior to being reviewed and approved by management and published.

Review of the testing schedule and continued applicability is reviewed on a regular basis and changes/adjustments are to be discussed with testing management before any modifications. All changes will be subject to review and challenge.

## Amendments to the Annual Testing Schedule

Changes or recommendations to the testing schedule must be reviewed and approved by the Testing Manager. A Schedule Change Request should be completed. The following information is to be included in the change request: the original plan start date and report issued dates, revise, start date and revised report, issuance state, justification for the change, approval by the testing manager, and the head of compliance.

All change requests will be subject to review and challenge by the head of testing and subsequent approval. Any disputes or concerns regarding schedule changes should be escalated up to the head of compliance.

Once the schedule change, request or request have been completed and approved a new schedule needs to be published and shared with the business units.

Changes to the testing schedule should be limited.

## Testing Execution

The testing team is responsible for ensuring all reviews are performed in accordance with the program standards. Once the review is completed, the testing manager is responsible for work paper review and retention.

**Workpaper Standards:** work papers are the documentation supporting the testing that was performed. Work papers should demonstrate clear trail of the steps performed, decisions, findings, observations and logic. A well-constructed test program will provide sufficient data to reconstruct the testers decision process for each step of the review. Adopt mutation should clearly support the reasons to include or exclusive, certain provisions of the regulations, laws, guidance, or business lines from the scope. It should also include adequate support for any findings or observations.

Templates have been designed and are in the appendix of this program. Templates allow for consistency among the testing work papers. Changes to a template are permitted to meet certain testing objectives, and to optimize the approach to testing.

**Testing Cycle:** the testing cycle is comprised of four phases: planning, fieldwork, reporting and quality control.

**Planning** – the planning phase is used to determine the key requirements, specific, scope, objectives, and timeline requirements of the review. The planning process takes into consideration adequacy of the design and effectiveness of controls if known. The planning phase further considers, identification of significant risks, associated and determination of the scope of the operations, policies, and procedures, including changes from the prior review.

The planning phase includes consideration of the optimal types of tests for the scope of the review, such as reviews of policies, procedures, key controls, as well as transactional testing. This phase involves consideration for processes, risks or requirements, not included in prior reviews. When planning and scoping the test, consider the risk to test. What different types of failure may occur for a given requirement, such as timeliness, accuracy, evidence population, and completeness. A scoping document should be used to capture the research completed and decisions made regarding the scope.

**Scoping Document** – the scoping document generally contains information about the topic being tested and helps to shape the scope and objectives of the test. Scoping document once completed is to be approved by the head of testing.

*Entrance Memo* – a testing memorandum should be prepared and distributed to the applicable, business partners, compliance partners, and other risk areas. This document provides a high-level overview of what is to be tested. It includes timing of the test, such as when it will start, and when it will be complete, an approximate date of when the report will be issued, and the names of the individuals who will be conducting the testing. The entrance memo should also include the dates and times of update meetings if being held. The scoping document should be attached to the Entrance Memo.

*Entrance Meeting* – once the entrance, memo has been distributed, a meeting should be scheduled with the appropriate business unit, line management, and compliance officers, and other applicable risk management staff.

**Fieldwork** – this is the phase where the work begins to assess the effectiveness of implementing controls to mitigate inherent risks of the areas being assessed. Or test, scripts or test work programs are utilized to assess the adequacy of the business unit. Detailed test scripts must be developed and align with the principles established by the fiduciary testing program. Depending on the type of review in the scope, the following should be included:

- Review the business unit organization charts, and obtain an understanding of roles and responsibilities within the business unit
- Review policies and procedures
- Review of prior examinations, internal audit reports other compliance, testing, and
- business unit monitoring activity
- Transaction testing
- Risk and control assessments
- Review training, materials

*Sampling Methodology* – Sampling methodology is used to select, verify, and test transactions and controls for the period covered by the review. The testing program should determine the objectives of testing, the procedures, to meet the objectives, and quantity of items to review.

When testers choose to test transactions, they should decide whether to use the statistical or non-statistical sampling methods. Testers can use non-statistical sampling for small populations when internal controls are effective, and it is not cost-effective to use statistical sampling. Testers can select statistical sampling method when quantification is appropriate, and they want to infer with certain degree of reliability and precision that the samples characteristics are indicative of the entire population.

The fiduciary testing program does not require the use of any specific methodology. Do use of sampling is left to the discretion of the tester. However, the methodology used should be justified and fully documented.



a) Determine the population for testing

The population from which the sample is drawn is driven by the test objective. The population includes items within the past 12 months or since the last test was performed.

b) Determine the sample size

Non-statistical – this approach is based on judgment and not derived through statistical sample size, determination, calculations, and random sampling. When it is not necessary to extrapolate the error rate to the entire population; non-statistical sampling, is best

Statistical samplings – if the tester has a well-defined population with common data elements and wants to project the error rate across the entire population, then statistical sampling is the preferred method

The tester must have reasonable assurance that the sample size is representative of the entire population when selecting the samples. Once the sample size is determined, the sample selection method is chosen.

c) Perform testing

<b>Inquiry</b>	Inquiry involves attaining, written, or oral information from the business unit in response to questions from the tester. Inquiry is not sufficient by itself and is to be used in conjunction with other kinds of corroborative evidence.
<b>Observation</b>	Observation is the visual assessment of a control. It is often used in conjunction with other kinds of corroborative evidence.
<b>Inspection</b>	The physical inspection and review of documents to verify the control effectiveness
<b>Reperformance</b>	Rechecking a sample of computation, or the process of a transaction from beginning to end

d) Issues

An issue is defined as identification of a control, gap, or absence of a control by the business unit, and other risk stakeholders, or those that are identified during an exam by internal audit, or a regulator.

e) Issue Ratings

Ratings should be based on conclusions about the adequacy and effectiveness of the business units controls to ensure compliance with applicable laws and regulations. The assigned rating also impact scope and frequency of future reviews. All risk ratings will be utilized to assist management and understanding the severity of the noted issues. The following elements should be considered, when determining the overall rating.

- Stability and experience of the business unit management and staff
- Adherence to establish policies and procedures
- Level of risk associated with findings
- Effectiveness of system, controls, quality assurance process, and methods to assess effectiveness.
- Actions taken to address prior regulatory exams, internal audit findings and other reviews and tests.
- Any proactive actions taken by management to address weaknesses in controls and self-identified issues.

The tester uses professional judgment when documenting the issue readings, and the overall review reading for the final report. All ratings must be justified and approved prior to being discussed with the business unit.

Identified issues are to be communicated to management via an issue memorandum. The issue memorandum must include a description of the issue that captures and state, the control deficiency or policy or procedure exception. The issue memo must also include the root cause any impact. Impact is the actual or potential outcome of the cause of an issue, resulting from an identified control, weakness or compliance weakness. Root cause is a description of the actual reasons why an expected outcome was not achieved.

#### Issue Ratings

High Risk	Issues that require immediate management, attention and correction. High probability of significant penalties or consequences reputation risk or curtailment of strategic initiatives.
Moderate Risk	Issues where timely management attention is warranted, but not immediate attention. Moderate rated issues can potentially lead to regulatory penalties or consequences if not corrected within a reasonable timeframe.
Low Risk	Low risk issues are those where the risk is limited, and routine management attention is warranted. These issues represent a potential risk such that if management does not act to correct, could evolve into a higher risk concern. Low risk issues also and tell a limited likelihood of penalties or other regulatory consequences.
Observation	An observation that does not pose an immediate compliance risk but may potentially result in an issue in the future if management does not address.

#### Types of issues identified

New - a new issue identified in the current test.

Repeat – an issue that was identified in a previous review, conducted by the second line fiduciary compliance testing.

Existing – previously identified, and which remediation is still underway during the current test.

**Reporting** – the test will conclude with a written Fiduciary Compliance Testing report summarizing the scope, compliance risks, findings, details of issues, corrective action and management’s response. The purpose of the testing report is to provide management with information on whether the business unit or activity tested is adhering to policies, procedures, applicable laws and regulations, if the controls are effective and the corrective action that management must take. Identified exceptions or advisory comments should be documented and both the issues memorandum and fiduciary compliance testing report. Once a draft report is issued, business management has 7 days to report concerns regarding the accuracy and contact before the final report is issued.

### **Final Report Content**

- *Executive Summary:*
  - **Background:** should provide general information on the regulation, activity, process being reviewed, and the business units applicability. Include any, and all relevant background information needed with respect to the purpose and objective of the review.
  - **Scope:** include the range of activities and period of transactions and records, subject to the test; and business units within the scope and the objective of the test
  - **Conclusion/Comments:**
    - i. Dissection summarizes the main trends and issues with the overall review rating, (strong satisfactory or needs improvement)
    - ii. Include issues if applicable, the issue total full description of the deficiency and any recommendations
- *Testing Results:*
  - Detailed summary of the testing results. Include background and description of the requirements tested.
  - Summarize the test steps needed to complete the review.
  - Summarize the conclusion of the test performed, including a summary of any issues
- *Summary of findings/issues/exceptions:*

- Description: factual statement, which captures the control deficiency or policy exception. This may include the number of exceptions identified, policy or procedure, exceptions, and violation of laws and regulations.
  - Root Cause: identify the actual or potential reasons why an expected outcome was not achieved.
  - Impact: the degree of exposure, resulting from an identified control or compliance weakness, is summarized in the section.
- *Overall Test Rating*:

Review ratings will be assigned to all fiduciary compliance testing reports. The assigned rating is based on conclusions about the adequacy and effectiveness of the business unit's compliance with applicable laws, regulations, policies and procedures. The assigned rating will effect the level and frequency of future testing. The following factors are considered when determining the rating:

- Adherence to policies and procedures
- Number and level of risk of any issues
- Level of collective risk associated with the findings
- Stability and experience of staff and management

The tester, testing lead and testing management use professional judgement when assigning the rating. The rating rationale must be included in the final testing report.

#### Fiduciary Compliance Testing Report Ratings

Rating	Definition
Satisfactory	Compliance practices and performance within the business unit and compliance with laws and regulations are satisfactory. No weaknesses were discovered during the review that indicated that applicable laws and regulations were not adhere to. Management maintains an effective control environment that provide reasonable assurance of compliance with applicable regulations, laws, policies, and procedures. There is appropriate management, oversight and training. Operating procedures, support the activities, business objectives. There may be some minor corrective actions required that can be managed in the normal course of business. It's
Needs Improvement	Compliance practices and performance within the business unit and compliance with laws and regulations under review need improvement. The control risk management and governance process contain several weaknesses that may prevent a business unit from achieving its business objectives.

	The review noted, exceptions and weaknesses that are considered high risk in nature or noted numerous moderate risk issues that collectively result in a high level of risk exposure. The high-risk issues noted in the review may lead to regulatory criticism enforcement, actions, fines, and could create reputation risk. Identified issues may also represent repeat findings that were either noted in prior compliance testing, internal audit, testing or regulatory examinations
Unsatisfactory	Are compliance practices and performance within the business unit contain critical or systemic deficiencies that can prevent not only the business unit from achieving its business objectives but also, it's strategic initiatives. Such weaknesses may not prevent the occurrence of significant risk exposure or material errors. The number and nature of the deficiencies require substantial management, attention and resources. Immediate, corrective action is required to prevent further deterioration.

**Quality Control** – This is the last phase of the testing execution. The quality control process is where a checklist is utilized to ensure that all the steps within the planning phase, the fieldwork phase, and reporting phase agree with established policy and procedure. The purpose of the quality control review is to ensure consistency across all of testing.

- Work papers and other supporting documents must be reviewed and approved by the testing lead and or manager prior to the final report being issued.
- Workpapers demonstrate a clear and sufficient trail of decisions and supporting logic and provide sufficient data to reconstruct the testers decision process.