



Trust and Wealth Management Audit Risk Strategies

Francis P. Thomas

The Glenmede Trust Company, N.A.

FIRMA's 29th National Training Conference

April 22, 2015 Nashville, TN

Disclaimer

The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of Glenmede. It is a general description of one company's strategy for internal audit. No single approach fits every organization.

As a regulated financial institution, Glenmede strives to ensure its fiduciary audit activities are conducted consistent with 12 CFR 9.9(b).

- *Continuous audit.* In lieu of performing annual audits under paragraph (a) of this section, a national bank may adopt a continuous audit system under which the bank arranges for a discrete audit (by internal or external auditors) of each significant fiduciary activity (i.e., on an activity-by-activity basis), under the direction of its fiduciary audit committee, at an interval commensurate with the nature and risk of that activity. Thus, certain fiduciary activities may receive audits at intervals greater or less than one year, as appropriate. A bank that adopts a continuous audit system shall note the results of all discrete audits performed since the last audit report (including significant actions taken as a result of the audits) in the minutes of the board of directors at least once during each calendar year .



Overview of Process

- Annual strategy session involving audit, compliance and risk management
- Populate the decision risk matrix
 - Define the Audit Universe
 - Choose the elements you want to risk evaluate
 - Establish your scoring methodology
 - Set the threshold score for considering an audit
 - Identify overdue assignments for priority scheduling
 - Leverage testing in other areas
 - Apply judgment for any resource constraints
 - Ensure the plan is achievable
 - Caveats for unforeseen situations



Define the Audit Universe

- Business units
 - Wealth Advisory (account administration)
 - Investment Management
 - Trade Processing
 - Investment Strategies
 - Securities Operations
 - Accounting and Finance
 - Sales and Marketing
 - Human Resources
- Functional areas
 - IT Management
 - Electronic Banking
 - Network Security
 - Outsourced Technology Services
- Identify areas with no audit activity
 - Dining Services
 - Legal
 - Corporate Secretary



Component Audits of a Wealth Advisory Review

- High Net Worth
 - Trust Accounts (revocable / irrevocable)
 - Investment Management Accounts (sole / shared)
 - Custody Accounts (no investment authority)
 - Charitable Trusts (Form 990 filings)
- Wealth Strategies (tax preparation / planning)
- Endowment and Foundation
- Specialized Fiduciary Services
 - Estate Administration
 - Administration of special / unique assets
 - Retirement Plans (EBT, IRA)
- Family Wealth Strategies

Risk Matrix Elements

- Changes in management since last audit report?
- Changes in systems or processes?
- Material changes to key personnel?
- Is there a third-party vendor involved in processing?
- How much time has elapsed since the last review?
- Were there any reportable items in last review?
- Any external or annual testing done (SOC-1)? **X**
- Have there been monetary errors?
- Is there any potential for misappropriation?
- Recent regulatory changes impact the process?
- Has a CSA been done in last 2 years? **X**

X = these can be viewed as enhancing a score

Scoring Methodology

- For questions with a yes or no answer,
 - yes = 1; no = 0
- For reverse thinking, e.g., is there a CSA*, or was SOC testing done, and you can review results then
 - tested without exception = <1>
 - not tested = 0
 - tested with exceptions noted = 1
- For questions such as “how long since last review,” we convert to fractional years. For example, 21 months gets recorded as 1.75 years.

* CSA - Control Self-Assessments



Leveraging Audit Testing

Service Organization Control reports can provide tests of the whole internal control structure and it is usually done annually to give you coverage in a wide range of business unit activity. When we test these key control areas for our external auditors, we also use the documentation for our internal purposes

- Account Administration
- Asset Pricing
- Reconciliation and Asset Safekeeping
- Fee Analysis
- Corporate Action processing
- Income Collection
- Securities Transactions
- System Reviews
- Client Reporting

Service Organization Control Reports

SOC Report Comparison

What they report on & Who uses them

	What it reports on	Who uses it
1	Internal controls over financial reporting	User auditors & users' controller's office
2	Security, availability, processing integrity, confidentiality or privacy controls	Management, regulators & others
3	Security, availability, processing integrity, confidentiality or privacy controls	Anyone

Source: OnLINE TECH.com (August 2011)

Control Self Assessment

If your risk or compliance team coordinates Control Self-Assessments (CSA) with a business unit, leveraging them for tests of key controls is very beneficial.

- Identify the “accountable manager” within the business unit as the subject matter expert for the topic.
- Define the scope. Reference laws, regs, policies, etc.
- Director of Risk Management facilitates discussion of the control environment, helping the user group identify key controls and whether they are measurable.
- Assess whether the control has monitoring and reporting, so that any control weakness is identified and escalated.
- Based on the monitoring’s effectiveness, identify areas for improvement, action plans to correct deficiencies, and a time window for implementation.
- Audit should ensure test programs can validate key controls and opine if they are adequate and consistently functioning.

Audit Cycle Definitions

- REGULATORY RATIONALE – despite the level of quality controls, some areas such as AML/BSA demand an annual review cycle.
- HIGH - with such risk levels, attempt to review every 12 to 18 months.
- VOLUNTARY – will be tested every year without respect to risk consideration (audit of bank's own pension plan).
- MEDIUM – moderately perceived risk, attempt to review every 19 to 30 months.
- LOW – a low risk area will be reviewed every 31 to 42 months.
- N/A – no cycle has been determined due to no or limited audit work being done in the area.
- NONE – if an audit is suspended due to inactivity (such as when securities lending is a strategy but not currently being done), then an audit will be shown with no cycle.

Information Technology Components of Trust Audits

Leverage every audit to the elements that are critical to today's risk analysis.

- Who has access to the trust accounting system? How many terminated people still have rights? Do non-employees/vendors have access rights?
- Who authorizes access? Is access site specific or can a user access remotely? Is documentation retained to evidence an approval process?
- Who reviews the people with system administration rights ("keys to the kingdom")?
- What edit rights (add, change, delete) are authorized within the function you are reviewing?
- Anyone take a look at what systems interface with trust accounting (uploads / downloads)? Could be the equivalent of an invisible user.
- Does anyone have the ability to change the software (modify the application program)?

Points to Ponder

- Have you ever considered soliciting business unit management input to tell audit “where to go?” This could help align your audit project plan with a value added service to management, assisting them where they want help.
- Once the project plan is approved by the Audit Committee, do you share it with management? Other than doing cash counts, is anyone conducting true “surprise audits?”
- Many organizations have some type of client complaint tracking, but let’s just see how many variations we have in this room on interpreting just what is a client complaint?
If management has not articulated in writing a common definition, is it reasonable to then test against a nebulous standard?



Questions, Comments, Ideas?

Francis P. Thomas
Managing Director / General Auditor
The Glenmede Trust Co., N.A.
Philadelphia, PA
Fran.Thomas@Glenmede.com
215-419-6040





Attendee Notes