AML Compliance
Risk Assessment and Testing

AIBA Quarterly Meeting
March 13, 2013
Agenda

1. AML Risk Assessment: The Purpose
2. Key Risk Factors
3. Mitigating Controls
4. The Risk Assessment Methodology
5. AML Compliance Testing
6. Conclusions and Recommendations
AML Risk Assessment: The Purpose

1. Identify inherent AML compliance risks of the bank, with particular emphasis on risks associated with products, geography (both international and domestic), and customer characteristics.

2. Assess the adequacy of controls that apply to the inherent risks.

3. The net or residual risks after the application of the controls.

4. The direction of risk.
Key Risk Factors

1. Product Risk

- Does the business offer wire transfers, cash activity, mobile banking, prepaid cards?
- Within the customer base, how many have one or more high risk products?
- Are there new products that have been introduced?

2. Geographic Risk

- Are customers located in any high risk countries? How many?
- Are customers located in high risk domestic geographies? How many?
- Do customers have transactions with counter parties in high risk countries? How many?
- Does the bank have offices in high risk countries or domestic locations? How many?

3. Customer Risk

- Does the bank have high risk customers? How many?
- Consumers: PEPs, aliens, certain occupations, other factors
- Businesses: foreign corporations, financial institutions, import/export companies
- Customers that were subjects of suspicious referrals
- Other criteria as defined by the bank
The mitigating controls to be assessed should include:

1. How effective are the controls that govern the risks of the business?

2. Controls would be pointed to each inherent risk category (product, geography, customer)

3. Controls include:
   - New customer reviews
   - Suspicious activity monitoring
   - Employee training
   - Processes performed by the business or centrally

4. High, medium or low criteria:
   - Audits
   - Examinations
   - Self identified issues
   - Judgment of AML Officer
1. The Compliance Risk Assessment ("CRA") process is used to assess the level of regulatory risk and evaluate the strength of controls.
   - Risks are assessed against applicable laws and regulations.

2. Risks are evaluated for each business/support group and the institution as a whole.

3. The CRA process drives the schedule for training, testing and the planning of future compliance activities (develop appropriate controls e.g., policy and procedures).

4. The finished CRA product is delivered to the Board of Directors and Federal Reserve.

5. Perform annually, or (1) as business changes (e.g. new products) or (2) on risk-based basis (e.g. high risk businesses are assessed more frequently).
The Risk Assessment Methodology (Cont.)

The CRA methodology includes 5 core action items:

1. Identify the business segments, business units and support functions to be assessed;

2. Determine scope of applicable compliance laws/regulations for business segment, business unit and support functions;

3. Score the Inherent Risk Factors and Control Strength Factors;

4. Generate Inherent Risk and Residual Risk Heat Maps; and

5. Draft the Compliance Risk Assessment Narratives.
1. **Inherent Risk:** The magnitude of a negative event based upon the nature and volume of business, the types of customers served by a particular business, and the risk of noncompliance of a particular compliance law or regulation.

2. **Control Factors:** Control factors may:
   - mitigate the level of inherent risk,
   - have no impact on the level of inherent risk, or
   - increase the level of risk in any business or group

3. **Residual Risk:** The risk remaining after the specific controls are calculated against the Inherent Risk. See the Residual Risk Matrix below.

<table>
<thead>
<tr>
<th>Inherent Risk</th>
<th>Strong Controls</th>
<th>Adequate Controls</th>
<th>Weak / Untested Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
</tbody>
</table>
Inherent Risk measures the risk with no consideration to the control environment. The Inherent Risk is determined by scoring multiple factors.

1. **Regulatory Environment** - Risk associated with changes to a law/regulation and the amount of attention the regulatory bodies are giving to determine whether there are any breaches.


3. **History of Problems** - Measures any issues raised regarding a particular regulation.

4. **Customer Complaints** - Complaints made by clients with respect to a compliance regulation.

5. **Level of Applicability to the Business** - How much a regulation relates to a particular business.

6. **Complexity and Interdependence** - How much of a process relies on another business, support functions within the corporation.
The Risk Assessment Methodology (Cont.)

7. **Reputation** - How reputation would be portrayed if institution failed to comply.
8. **Country Profile** - The country where business is conducted.
9. **Type of Customer** - The type of the customer of the business.
10. **Business Growth** - The risk associated with the growth of the business.
12. **Outsourcing** - The risk associated with outsourcing or reliance on third-party providers to perform services on behalf of an institution.
13. **Staffing** - The risk associated when staffing levels are not up to the level needed.
14. **Staffing Turnover** - The risk associated with turnover.
Independent testing of the overall compliance program is one of the four pillars of an effective AML Program. It is designed to evaluate the integrity and effectiveness of the program. The goal is to:

1. Reduce money laundering and/or terrorist financing risks

3. Anticipate requirements of AML/BSA exams

5. Identify deficiencies of the AML Program
Test the established internal controls.

1. Accuracy and timing of reports (SARs, Incident Reports)
2. New Account KYC and CIP procedures
3. OFAC procedures
4. Transaction Monitoring System
5. Clearing and escalating of alerts
6. Effectiveness of employee AML training program
7. Test sample customer files and transactions against regulatory requirements and the Bank’s policies and procedures
8. Periodic and timely review of accounts including all medium and low risk relationships
The “Not So” Effective Audit Program

1. Frequency and Scope of the Audits are not Based on Risk within the Business Unit
   - Foreign private banking accounts are reviewed with the same frequency as domestic private banking accounts.
   - Areas not integrated to automated monitoring processes are subject to limited transactional testing.

2. Limited and Insufficient Testing
   - Testing programs are copied from last year's review and do not address significant changes to the processes (e.g., implementation of automated systems).
   - Reviews limited to interviews and walkthroughs without testing controls.
   - Automated monitoring systems' parameters not tested for effectiveness.
   - The SAR process is limited to a “reasonableness and completeness” review that only includes the files that were actually filed, without thoroughly testing the detection and monitoring processes.
   - Exclusion of higher-risk activities as part of the testing.
AML Compliance Testing (Cont.)

The testing program must ensure the following:

1. The scope is documented;

2. The review process is documented;

3. Whether the review has identified any weaknesses; and

4. The results, including any corrective actions, are documented.
AML Compliance Testing (Cont.)

**AML Controls**

Establish appropriate policies and procedures to adequately identify the identity of the client, the beneficial owners, senior political figures (PEPs) and assess the

Establish monitoring processes to ensure that the risk profile is periodically reviewed.

Establish comprehensive policies, procedures and mechanisms to timely and appropriately escalate unusual activity.

**Example of Testing Procedures**

1. Are there adequate policies and procedures?
   Review policies and procedures and determine if they include all regulatory requirements and clearly delineate BNY’s policies and procedures.

2. Are customers’ files complete?
   Test a sample of customer files and determine whether they comply with regulatory requirements as well as BNY’s internal policies and procedures.

1. Is the customer risk profile periodically reviewed?
   Test a sample of files and determine whether the risk profile has been appropriately and periodically reviewed.

1. Are there adequate policies and procedures?
   Review policies and procedures and determine if they adequately establish mechanisms to timely and appropriately escalate unusual activity.
Conclusions and Recommendations

1. Conclusions
   a. Do the controls adequately manage each inherent risk category?
   b. Can the net product, net geography and net customer risk be rolled up into a net AML risk rating for the bank?
   c. Expert judgment must be used to ultimately apply the risk rating
   d. Apply direction of risk (increasing, stable or decreasing)

2. Recommendations
   a. Large institutions with varying businesses should consider “rolling up” the bank-wide risk profile
   b. The Risk Assessment should be performed:
      • Annually, or
      • As business changes (e.g. new products)
Thank You

Thomas Bock, Managing Director

K2 Intelligence
(917) 243 - 7304
tbock@k2intelligence.com