Meet the Team: Mary Presberg

Mary Presberg
Partner/Principal, PwC Advisory
mary.k.presberg@pwc.com

- Mary is a Principal in PwC’s Financial Crimes Unit in the Chicago office
- Over 16 years of industry experience working with leading financial services firms across areas such as heightened regulatory standards, corporate governance, risk management, risk appetite, internal controls and regulatory management
- Project experience includes:
  - Leading the design of target operating models, program governance and escalation frameworks
  - Conducting fraud and BSA/AML threat assessments
  - Leading programs to streamline operations processes to comply with current regulatory standards and expectations
  - Leading gap analyses of existing compliance and BSA/AML programs, and addressing regulatory enforcement actions
- Prior to joining PwC, Mary worked as a fixed annuity manager at a large financial services firm managing cross-channel product launches, which included product development, leading product approval negotiations with the state departments of insurance and the SEC, and designing technology implementation solutions for new product designs
Meet the Team: Thomas Cahuzac

Thomas Cahuzac
Manager, PwC Advisory
thomas.cahuzac@pwc.com

- Thomas is a manager in PwC’s Financial Crimes Unit
- Primary focus includes developing risk assessment methodologies and associated workflows, as well as business requirements for tool development.
- Thomas has also managed teams to execute the BSA/AML and Sanctions and ACG Risk Assessments on a global scale, and design periodic review processes. Project experience includes:
  - Managing the team executing RA, developing set of BRDs for products and wire data, and developing QA process.
  - Developing workflows and defining roles and responsibilities
  - Designing a gap analysis of current NNS alert review processes followed by regional and global AML teams. Analyzing RDC alert generation and drafting procedures to reduce alert review by 30%.
  - Drafting periodic review procedures and developing screening procedure analysis to enable a clear view of screening system effectiveness and overlap.
  - Managing local and global teams to develop and execute a process to automate and generate monthly and quarterly global governance metrics and reporting.
Agenda

1. BSA/AML and Sanctions Themes & Challenges
2. Regulatory Expectations
3. BSA/AML and Sanctions Risk Assessment Expected Outcomes
4. Considerations and Perspectives
5. Risk Assessment Approach
6. Data Sourcing and GRC/Risk Assessment Solution
7. Recap & Key Takeaways
BSA/AML and Sanctions Themes & Challenges

What are some general themes that we are seeing today?

1. **The new regulatory environment**
   Heightened regulatory standards and expectations continue to impact the financial services industry. Sanctions continue to evolve to match global risk. Regulators are scrutinizing institutions’ ability to prevent financial crime and proactively manage risk through data and analysis. Over a dozen global financial institutions have been assessed fines in the hundreds of millions to billions of dollars for money laundering and/or sanctions violations.

2. **The revolution in information**
   Data is growing in volume, variety, and velocity, and the ability to harness data as a strategic asset is critical.

3. **Continued vulnerability of institutions to bad actors**
   Criminals and organizations are finding new ways, both high and low tech, to evade institutional controls that would prevent the laundering of funds from illicit activities and the movement of funds by sanctioned individuals/entities.

4. **Culture of compliance**
   Shift from a forced reactive mode, focused on addressing regulatory matters and addressing issues as they arise, to a proactive identification of trends and development of program strategy. This is also apparent with the newly developing 1st and 2nd LOD interaction models (1L) and second line (2L) integration, which clarifies ownership and better balances competing priorities, risk, cost, and benefits.

Five ways to manage anti-money laundering and sanctions challenges:

1. **Know your customer**
   Ensure the customer due diligence (CDD) rule requirements are implemented seamlessly across the entire global institution.

2. **Clear support from management**
   Leadership should create a culture that supports a culture of compliance that enables a strategic approach and investment mitigating the risk.

3. **Changes in the environment**
   Institutions need to stay educated on the ways in which bad actors utilize their institutions to launder money (e.g., new schemes, both high and low tech).

4. **Conduct risk assessments**
   Assess risks not only within your institution but also your third-party relationships.

5. **Up-to-date technology**
   Having data-driven and analytically capable platforms can help institutions move from a cumbersome manual process to a more strategic and efficient approach.
From planning to reporting ... all the stars must align to create the perfect Risk Assessment picture ...
Regulators in the United States, Europe and Australia have imposed $342 billion of fines on banks since 2009 for misconduct, including violation of anti-money laundering rules, and that is likely to top $400 billion by 2020.

**Jan 31, 2017**

Deutsche Bank fined for $10 billion Russian money-laundering scheme

The giant German lender was hit with about $630 million in penalties on Tuesday over a $10 billion Russian money-laundering scheme that involved its Moscow, New York and London branches.

**Feb 15, 2018**

U.S. Bancorp to Pay $528 Million for Subsidiary’s AML Failures

The U.S. Justice Department entered into a deferred prosecution agreement with the Minneapolis, MN-based banking holding company on behalf of its Cincinnati, OH-based subsidiary requiring it to pay a $528 million penalty and continue reform of its BSA and AML compliance.
Regulators in the United States, Europe and Australia have imposed $342 billion of fines on banks since 2009 for misconduct, including violation of anti-money laundering rules, and that is likely to top $400 billion by 2020.

**Australia’s Largest Bank Agrees to Historic AML Penalty**

Commonwealth Bank of Australia (“CBA”), has agreed to a proposed civil settlement — subject to court approval — of historic proportions, involving a fine of approximately $700 million Australian dollars regarding numerous alleged Anti-Money Laundering (“AML”) and Counter Terrorism Financing (“CTF”) violations.

**Citibank fined $70 million for anti-money laundering compliance shortcomings**

A U.S. bank regulator has fined Citibank (C.N) $70 million for failing to address shortcomings in its anti-money laundering policies.
Summary of analysis of key USA fines and assessments for AML between 2008-2016 and common recurring themes identified for Risk Assessment deficiencies:

- Failure to have an overall adequate risk assessment
- Failure to have an enterprise wide risk assessment
- Failure to assess risk exposure within the context of products, services, customers, transaction types or geographical reach of the institution
- Ineffective Risk rating process. Lack of understanding of basic AML requirements resulted in failure to identify, evaluate and risk rate dozens of higher risk accounts to mitigate potential AML risks
- Failure to periodically review risk rating process to ensure that all high-risk customers were identified

Source: USA AML Fines 2008 – 2016
Regulatory Expectations

Develop actionable items from identified risks

The BSA/AML and Sanctions Risk Assessment is a pillar of a financial institution's annual compliance planning.

Execute on a detailed and documented methodology

Methodology must be detailed and well documented. Process must be reproducible and a detailed audit trail must be kept (e.g., procedure, workflows, roles & responsibilities, data sourcing, system flows, and etc.)

Incorporate qualitative as well as quantitative components

A successful risk assessment must incorporate accurate customer, product, and geography data and also incorporate qualitative components provided by each individual assessment unit*

Develop and refine a repeatable process which considers YoY trends

Data from previous years must be available to enable YoY analysis (which should also include other related metrics and reporting, trends and regulatory findings)

*Assessment Unit can include different levels of granularity, including but not limited to business units, products, local and global jurisdictions, etc.
Gathering Data for Risk Assessment

USE THE CRS DATABASE TO SIZE THE MARKET.

THAT DATA IS WRONG.

THEN USE THE SIBS DATABASE.

THAT DATA IS ALSO WRONG.

CAN YOU AVERAGE THEM?

SURE. I CAN MULTIPLY THEM TOO.
BSA/ AML and Sanctions Risk Assessment ("RA") Objectives

Move the needle from a check the box exercise that includes development of a detailed 100 page report, read only by internal audit and signed off by key stakeholders, to ... understanding your institution’s real AML and Sanctions risks, and enabling meaningful action to mitigate identified risks.

**From:** 100 pages of detailed documentation with no emerging themes or trends

**To:** Understanding your institution’s real BSA/AML and Sanctions risks, and enabling meaningful action to mitigate identified risks

- Enhance compliance planning, with effective allocation of resources
- Identify exposure to BSA/AML and Sanctions risk to address related controls
- Identify risks requiring immediate action and monitoring
- Develop a forum to review the institution’s BSA/AML and Sanctions risk amongst the three lines of defense
- Provide effective reporting to management around current and emerging BSA/AML and Sanctions risk
## Considerations and Perspectives

<table>
<thead>
<tr>
<th>Consideration</th>
<th>Description</th>
<th>Perspective</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Culture of Compliance</strong></td>
<td>• The risk assessment fosters a partnership between the business and compliance. Often times, there is a disconnect between compliance and front office staff. This leads to a breakdown, where compliance is not knowledgeable of the business conducted in an institution and front office staff is not aware of the BSA/AML and Sanctions risks inherent in their business.</td>
<td>• A well-rounded risk assessment should have close collaboration between compliance and the business through all stages (planning, execution, reporting). Teams should proactively assess the business and identify areas of higher compliance and regulatory risk informed by higher risk customers, products, and geographies. This will help the business better navigate through the risk and also improve Board-level communication.</td>
</tr>
<tr>
<td><strong>Methodology</strong></td>
<td>• There is no required method or format for completing a risk assessment. A financial institution should implement an appropriate methodology based on factors such as its size, organization, global exposure and risk appetite.</td>
<td>• At its core, the risk assessment can be viewed as a three step process where it should (1) identify all relevant inherent BSA/AML and Sanctions risks that a financial institution is facing, (2) assess the nature of mitigating controls, and (3) establish the residual risk that remains for the financial institution.</td>
</tr>
<tr>
<td><strong>Risk Appetite</strong></td>
<td>• BSA/AML and Sanctions Risk Assessment should be an integral part of the financial institution’s overall risk appetite. BSA/AML and Sanctions risks are an important part of the institution’s overall compliance and regulatory risk.</td>
<td>• The risk assessment must be constructed in a way that compliance can easily feed this information into the financial institution’s overall risk appetite and risk management solutions. Areas with high residual risk should be reviewed to identify ways the risk may be lowered or managed.</td>
</tr>
<tr>
<td><strong>Data Availability</strong></td>
<td>• The objective of every financial institution should be to adopt a quantitative approach when measuring inherent risk levels in the course of conducting a risk assessment. However, the acquisition and usage of quantitative data can be more of an art than a science.</td>
<td>• In the event that certain data elements are difficult to procure, the financial institution should utilize data proxies in their stead. While there is no prescriptive approach to employing data proxies, the surrogate factors should be representative of the data elements that they are replacing.</td>
</tr>
<tr>
<td><strong>Data Visualization</strong></td>
<td>• Due to the vast amount of data available at most financial institutions, the data acquisition will offer a plethora of information that may be too large to present at a high level. Using data visualization tools allows for bulky data sets to coalesce into visually simple, yet powerful graphics.</td>
<td>• The complex interactions of thousands of data points can be shown at once allowing the user to observe any overarching trends that may be too subtle to notice in the underlying data alone. Such data visualization tools offer a dynamic interface that allows the user to easily control what subsets of data should be considered for rendering a graphic display.</td>
</tr>
<tr>
<td><strong>Assignment of Risk</strong></td>
<td>• Once the BSA/AML and Sanctions risks of different customers, products, and geographies are identified, it is important to determine which part of the business will own the risk.</td>
<td>• Financial institutions must be clear in the way that they place risk within their organization because inaccurate placement can undermine efforts to accurately mitigate and manage BSA/AML and Sanctions risk.</td>
</tr>
</tbody>
</table>
BSA/AML and Sanctions RA Operating Model

Developing a fit-for-purpose BSA/AML and Sanctions Risk Assessment operating model will help bolster the Culture of Compliance and provide the organizing logic to strategically define and manage organization, people, process, and technology capabilities.

1. **Strategy:** As the cornerstone of a BSA/AML and OFAC program, the risk assessment needs to have a clearly defined strategy along with a cohesive organizational structure across compliance (2nd line) and the business (1st line). This will drive the vision and bolster the culture to proactively assess the risk appetite and profile across your institution.

2. **Functions:** Your institution's BSA/AML and Sanctions Risk Assessment functions should be understood among all stakeholders. The risk exposure and appetite from the strategy will help inform the scope of the risk assessment methodology and corresponding functions. Frequent interactions between the 1st and 2nd lines are key during development and execution to prevent any surprises and clarify risk assignments.

3. **Tech & Data:** Data is the lifeblood that runs through a risk assessment. It is important that your institution's data sourcing is confirmed and quality is acceptable. Having bad data will mislead your risk scoring. Based on your organization size, you should also move away from manual surveys and centralize in a RA tool.
The Risk Assessment involves five key phases. After the initial preparation and planning for the assessment, the inherent risk and control environment assessments are conducted. The residual risk rating is then calculated using the inherent risk and control ratings as inputs. Management reviews and acknowledges all ratings determined during the risk assessment.
Phase 1 - Scope and Planning

Scope and Planning is a critical phase for the success of the risk assessment.

- Determine scope
- Define Roles & Responsibilities
- Define Assessment Units
- Identify data sources and contacts
- Collect data and documentation
- Conduct AU interviews
- Review and update methodology
- Prepare surveys and back end support

Considerations/Lessons Learned

- **When defining roles and responsibilities:**
  - Consider whether users have the necessary knowledge
  - Consider whether user has access to the pertinent information/data
  - Consider the total work effort and whether multiple users will be leveraging the same information

- **When defining Assessment Units:**
  - Consider new products and the unique risks associated to existing products
  - Consider whether substantive changes to the business structure have occurred

- **Plan ahead!**
  - Consider what will be needed within the surveys during each phase of the risk assessment
  - Consider completeness and QA functionalities
Phase 2 - Inherent Risk Assessment

The Inherent Risk Assessment phase involves creating the risk assessment model, organizing the data provided, and analyzing the data to determine the inherent risk scores and ratings. Results are shared with the institution’s AML Risk Assessment team to obtain input and resolve any discrepancies.

- Implement the risk assessment methodology and organized data
- Conduct inherent risk assessment
- Share and refine results with applicable regional/global stakeholders

Considerations/Lessons Learned

- Reuse existing firm taxonomy as appropriate
  - Do not reinvent the wheel unless deemed necessary
- Confirm whether data is comprehensive
  - Establish a complete list of systems
  - Ensure you have an understanding of system scope/limitations (e.g. enterprise-wide, local, etc.)
- Ensure consistency across all data reported by all stakeholder groups
  - Create a glossary of terms and agree with stakeholder groups
- Consider all related metrics and reporting
  - Review within your institution to ensure results are consistent across programs including, regulator reporting
In the Control Environment Assessment phase, control processes are analyzed for effectiveness. A control environment rating is determined for each assessment unit. Results are shared with the institution’s AML Risk Assessment team.

- Review control processes and procedures
- Determine/calculate a control environment score for each assessment unit
- Share and refine results with applicable regional/global stakeholder

Considerations/Lessons Learned

- Consider different levels of automation and controls (from low to high tech)
- Consider whether controls are performed by a central group or by individual teams
  - Ensure that appropriate users are completing the survey, and consider pre-populating the information
  - Define terms and provide guidelines to the user (e.g. define manually, automated, etc.)
  - Avoid using responses and terms that are open ended and not specific (e.g. usually, often, etc.)
Levels of Automation Considerations:

Risk Ranking:

- **Level 1**: A process is not in place to determine the risk for all customers and entities.
- **Level 2**: A manual process is in place to determine the risk rating for all customers and entities.
- **Level 3**: An automated process is in place to determine the risk rating for all customers and entities.

Transactions for Products/Services:

- **Level 1**: Some transactions for products/services are not surveilled under an AML transaction surveillance system. No manual process is in place to review remaining product transactions.
- **Level 2**: Some transactions for products/services are not surveilled under an AML transaction surveillance system. However a manual process is in place to review product transactions.
- **Level 3**: All transactions for products/services are surveilled under an AML transaction surveillance system.

Screening Logic Generating Actimize Alerts:

- Level 1: Exact match only is used to screen customer names against Politically Exposed Person/Negative News databases.
- Level 2: Partial match and exact match logic are used to screen customer names against Politically Exposed Person/Negative news databases.

Note: Process automation can result in considerable time savings. These can be achieved through system workflow automation or through the development of "simple" processes such as Excel macros or Robotic Process Automations (RPAs).
Phase 4 - Residual Risk

Once inherent risk and control environment ratings are determined, residual risk ratings are calculated for each assessment unit. Results are reported to assessment unit leaders, who review and acknowledged the ratings for their respective assessment unit.

- Calculate residual risk using inherent risk and control environment ratings
- Obtain sign-off from business leaders, acknowledging all ratings for their assessment units

Considerations/Lessons Learned
- Clearly define application of overrides and employ a disciplined approach to timely and thorough documentation requirements
- Ensure that the final ratings provide an accurate depiction of your institution’s current risk profile
  - Your ratings could be grossly flawed because of the segmentation logic that was used to define the assessment units
Phase 5 - Reporting

Once the assessment is completed and sign-off is obtained from each assessment unit, the results have to be aggregated at the branch level and reported to client management.

Scope and Planning  Inherent Risk Assessment  Control Environment Assessment  Residual Risk  Reporting

- Aggregate and report results to senior management
- Document lessons learned and methodology

Considerations/Lessons Learned

- Provide a comprehensive view of your institution’s BSA/AML and OFAC risks
  - Provide the reader with an overall picture of the risks while also assessing the risks at a granular level
  - Must construct a clear picture of the BSA/AML and OFAC risks by customers, products and geographies
- Must include actionable items to mitigate overall residual risk
Once the assessment is completed and sign-off is obtained from each assessment unit, the results are aggregated and escalated to the appropriate stakeholders. Action plans must be developed at the different levels of granularity based on the resulting inherent risk, controls and residual risk ratings.
Data Sourcing and GRC/Risk Assessment Solution: Overview

**Data Sourcing**
Data sourcing and quality are essential for a sound risk assessment program. There should be a focus on data requirements, critical data elements (CDE), and usage for risk assessment purposes in order to determine data sources.

**Central Data Repository**
Data from various source systems should be aggregated into a central data repository to reduce point-to-point sourcing. Appropriate data quality checks and controls should be implemented at the ETL level to help ensure consistent data quality.

**Extract Transform and Load Data**

**GRC/Risk Assessment Tool**
- Intuitive UI
- Business Rules & Workflows
- Analytics & Reporting
- Audit & Data Access Control
- Dashboards
- Permissions/Entitlements

**Tool**
The tool should integrate with the Central Data Repository and load data structured to methodology requirements; reducing the need to “cut” data outside of a centralized tool.

*Start with “why” and the end in mind to design your user experience that aligns with your strategy and vision.*

*Deliver results in an agile manner through continuous collaboration and refinement among business, compliance, and tech stakeholders.*
Data Sourcing and GRC/Risk Assessment Solution: Benefits

1. **Automation**
   - Reduce manual errors, improves quality of results and helps ensure repeatable execution

2. **Data Access Control**
   - Maintains a history of actions taken by risk assessment users and eliminates version control issues

3. **Data Analytics & Reporting**
   - Integrated analytics, visualization, and reporting to draw insights and trends around your institution’s risk

4. **Cost and Time Saving**
   - Free up resources to focus on strategic and higher value parts of the risk assessment

5. **Central Data Repository**
   - Aggregation of data from multiple sources into a single repository allowing for easy access and management
Recap and Key Takeaways

Collaborate! Work closely with the business throughout your risk assessment process to foster a shared vision and understanding of your institution’s risk

**From:** 100 pages of detailed documentation with no emerging themes or trends

**To:** Understanding your institution’s real BSA/AML and Sanctions risks, and enabling meaningful action to mitigate identified risks

Plan ahead! Define your approach, roles and responsibilities, and methodology carefully

From great data, comes great results! Identify your data requirements and sources diligently to help ensure accuracy and completeness

Automation can be as simple as a macro! Consider automation to improve your process, decrease manual errors, and increase efficiency
For more information

Mary Presberg
PwC | Principal
Mobile: +1 312.231.0459
Email: mary.k.presberg@pwc.com

Thomas Cahuzac
PwC | Manager
Mobile: +1 646.455.8860
Email: Thomas.cahuzac@pwc.com