



KPMG FORENSIC<sup>SM</sup>

# Anti-Money Laundering Audit & Compliance Forum ("AMLAC")

**Pre-Conference Workshop:  
*Developing an Effective Risk-  
Based Compliance Program***

# Presenter

## ◆ Darren Donovan, *Principal*, KPMG LLP, Forensic Services

- Certified Fraud Examiner (CFE)
- Certified Protection Professional (CPP)
- Member, American Bar Association, White Collar Crime Section
- Member of ASIS National Standing Committee on Economic Crime
- Extensive experience in the areas of financial fraud, due diligence and anti-money laundering

# Workshop Learning Objectives

## Focus on BSA/AML Risk Assessment:

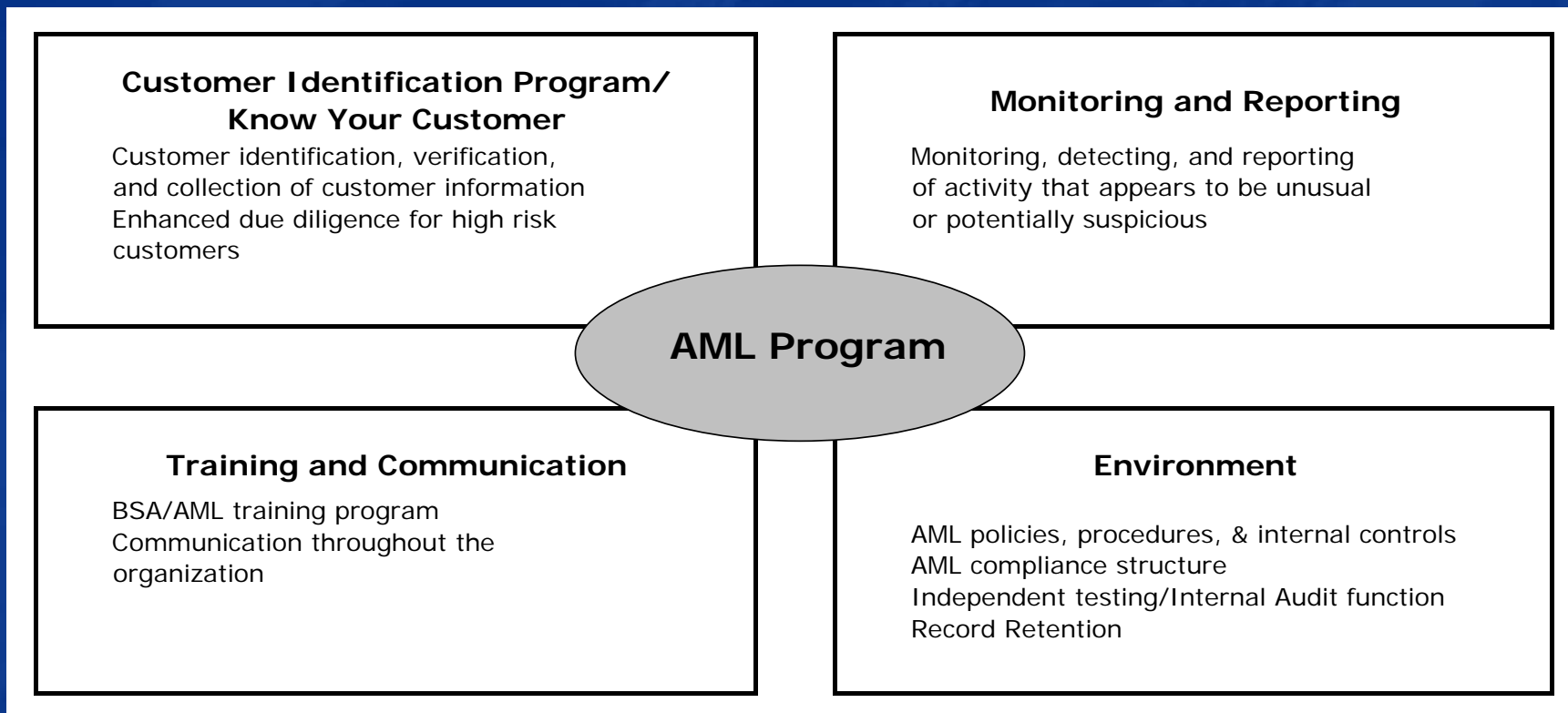
- ◆ Define the BSA/AML risk assessment process
- ◆ Learn how to build a bank's risk profile
- ◆ Learn how to analyze specific risk categories
- ◆ Understand how to implement an enterprise-wide BSA/AML risk assessment program

# Key Acronyms

<b>AML</b>	Anti-Money Laundering
<b>BSA</b>	Bank Secrecy Act
<b>CDD</b>	Customer Due Diligence
<b>FATF</b>	Financial Action Task Force
<b>FinCEN</b>	Financial Crimes Enforcement Network
<b>HIDTA</b>	High Intensity Drug Trafficking Areas
<b>HIFCA</b>	High Intensity Financial Crime Areas
<b>OFAC</b>	Office of Foreign Assets Control
<b>PEP</b>	Politically Exposed Person
<b>USA PATRIOT Act</b>	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001

# The Key Elements of an AML Program

The key elements of an effective risk-based AML Compliance Program are set out below:



# Managing Your Risks

## A. *Risk-Based Approach*

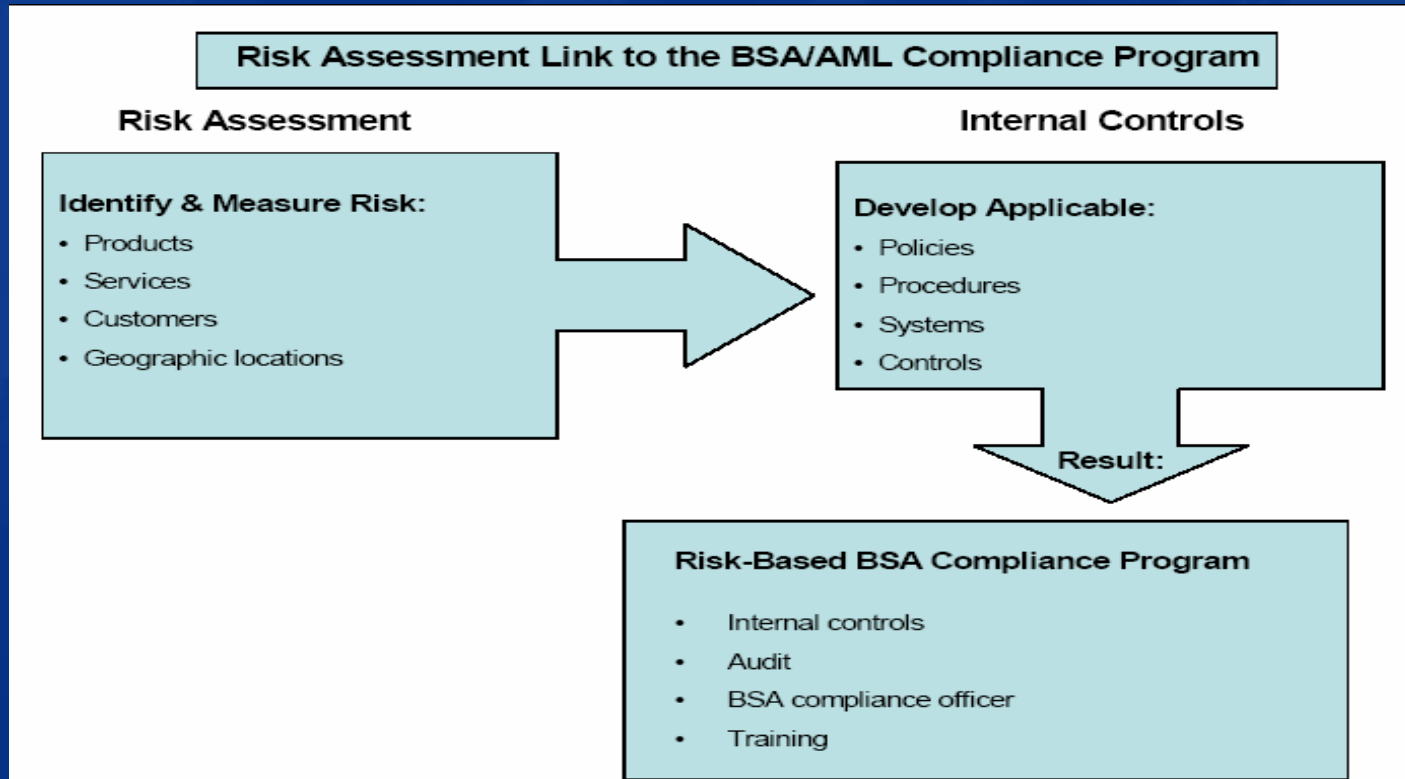
### ◆ Utilization of a Risk-Based Approach

- Risk is taken into consideration at both:
    - The beginning of a customer relationship
    - During the life of the relationship
  - Development, implementation, and updating of a risk matrix to assess a specific level of risk for each situation
  - A bank's risk profile will vary from one bank to another
- Examples of risk rating scores include:
- Low, Medium, High
  - Low, Low/Medium, Medium, Medium/High, High
  - Neutral, High

# Managing Your Risks

## A. Risk-Based Approach

Appendix I of the FFIEC's BSA/AML Examination Manual depicts how a bank's risk assessment is linked to the bank's BSA/AML compliance program:



# Managing Your Risks

## ***B. BSA/AML Risk Assessment***

### **1. Risk-Based Approach: *Understanding Your Risks***

#### ◆ **Two-step approach to BSA/AML Risk Assessment:**

**1. Identification Stage:** Identify specific variables unique to the bank within each of the following categories:

- Products and Services
- Customers and Entities
- Geographic Locations

**2. Analysis Stage:** Analysis of specific risk factors, including:

- Number and volume of transactions
- Geographic location
- Nature of the customer relationships
- Purpose of the account

# Managing Your Risks

## *B. BSA/AML Risk Assessment*

### *2. Risk-Based Approach: Products & Services Risk*

#### 1. Identification Stage

- ◆ Monetary instruments and wires for non-customers
- ◆ Trust accounts
- ◆ Transactions involving a financial intermediary where the beneficiary is undisclosed
- ◆ Products involving the electronic movement of funds with a cross border or foreign exchange component
- ◆ Wire transfers
- ◆ Private banking type of accounts
- ◆ Correspondent banking with offshore banks or banks located in high-risk jurisdictions
- ◆ Payable-through accounts
- ◆ Concentration accounts
- ◆ Private investment companies
- ◆ Loans secured by deposits at Foreign Financial Institutions
- ◆ Cash Letter and Pouch services
- ◆ Safe deposit box

# Managing Your Risks

## B. BSA/AML Risk Assessment

### 3. Risk-Based Approach: *High-Risk Industries*

#### 1. Identification Stage – Cont'd

##### Service Providers

- ◆ Broker dealers
- ◆ Travel agencies
- ◆ Sole practitioners
- ◆ Pawn brokers
- ◆ Real estate brokers/agents
- ◆ Ship/bus/airplane operators

##### Cash-Intensive Businesses

- ◆ Convenience stores
- ◆ Parking garages
- ◆ Restaurants

##### Gaming

- ◆ Casinos
- ◆ Gaming establishments
- ◆ Card clubs

##### Wholesalers/Retailers

- ◆ Consumer electronics (particularly in free trade zones)
- ◆ Leather goods stores
- ◆ Textile businesses
- ◆ Import-export/trading companies
- ◆ Car/boat/airplane dealerships
- ◆ Used automobile/truck/machine parts manufacturers
- ◆ Costume jewelry exporters
- ◆ Jewel/gem/precious metal dealers
- ◆ Arms dealers/arms manufacturers

##### Other

- ◆ Art & Antique dealers
- ◆ Auctioneers
- ◆ Charities/foundations/religious organizations
- ◆ Telemarketers

# Managing Your Risks

## ***B. BSA/AML Risk Assessment***

### ***4. Risk-Based Approach: Business & Entity Risk***

#### **1. Identification Stage – Cont'd**

##### **A. Non-Bank Financial Entities**

- Currency exchange houses
- Money transmitters
- Check cashing establishments
- Pawn brokers

##### **B. Banks**

- In areas designated as high intensity drug trafficking areas by the U.S. Office of National Drug Control Policy (For example, Houston, Los Angeles, New Jersey/New York, Miami, Southwest Border, Washington/Baltimore, Puerto Rico/ U.S. Virgin Islands)

##### **C. Financial Institutions and Legal Vehicles**

- Offshore banks, trusts, and private investment companies that offer confidentiality and intermediary services
- Offshore subsidiaries of corporations and banks located in secrecy jurisdictions and/or tax havens

# Managing Your Risks

## ***B. BSA/AML Risk Assessment***

### ***4. Risk-Based Approach: Business & Entity Risk – Cont'd***

#### **1. Identification Stage – Cont'd**

##### **D. Professional Service Providers**

- Accountants, lawyers, trustees and notaries that may be involved in facilitating the layering and integration of assets
- Non-Governmental Organizations (“NGOs”)/ Charities

##### **E. Politically Exposed Persons (“PEPs”)**

- Consulates/Embassies/Foreign Government Entities
- Non-Resident Aliens (“NRAs”)

# Managing Your Risks

## B. BSA/AML Risk Assessment

### 5. Risk-Based Approach: *Geographic Location Risk*

#### 1. Identification Stage – Cont'd

- International high-risk geographic locations include:
  - Countries subject to OFAC Sanctions
  - Countries identified as supporting International Terrorism (under Export Administration Act of 1979)
  - FATF's Non-Cooperative Countries and Territories ("NCCT")
  - Major money laundering countries identified by the International Narcotics Control Strategy Report ("INCSR")
  - Offshore Financial Centers ("OFCs")/ Bank Secrecy Havens ("BSHs")
  - Jurisdictions determined to be "of primary money laundering concern" by the Secretary of the Treasury, and jurisdictions subject to special measures imposed by the Secretary of the Treasury, pursuant to Section 311 of the USA PATRIOT Act

# Managing Your Risks

## *B. BSA/AML Risk Assessment*

### *5. Risk-Based Approach: Geographic Location Risk*

#### 1. Identification Stage – Cont'd

- Domestic high-risk geographic locations include:
  - High Intensity Drug Trafficking Areas (“HIDTAs”)
  - High Intensity Financial Crime Areas (“HIFCAs”)

# A Closer Look at HIDTA-Designated Counties

- ◆ **HIDTA-designated counties comprise approximately 13% of U.S. counties, represented in 43 states, Puerto Rico, the U.S. Virgin Islands, and the District of Columbia. The following 28 areas are designated as HIDTAs:**
  - **1990:** Houston, Los Angeles, New York/New Jersey, South Florida and Southwest Border (California, Arizona, New Mexico and Texas);
  - 1994: Washington/Baltimore (Maryland, Virginia and District of Columbia) and Puerto Rico/U.S. Virgin Islands;
  - **1995:** Atlanta, Chicago and Philadelphia/Camden;
  - **1996:** Rocky Mountain (Colorado, Montana, Utah and Wyoming), Gulf Coast (Alabama, Louisiana and Mississippi), Lake County (Indiana), Midwest (Iowa, Kansas, Missouri, Nebraska, North Dakota and South Dakota) and Northwest (Washington State);
  - **1997:** Southeastern Michigan (subsequently, portions of western Michigan) and Northern California;
  - **1998:** Appalachia (Kentucky, Tennessee and West Virginia), Central Florida, Milwaukee and North Texas (Texas and Oklahoma); and
  - **1999:** Central Valley California, Hawaii, New England (Connecticut, New Hampshire, Maine, Massachusetts, Rhode Island and Vermont), Ohio and Oregon.
  - **2001:** North Florida and Nevada.

# Managing Your Risks

## ***B. BSA/AML Risk Assessment***

### **1. Risk-Based Approach: *Understanding Your Risks***

## **2. Analysis Stage**

- Conduct a more detailed analysis of the original data obtained during the identification stage
- Accurately assess BSA/AML risk of data pertaining to the bank's activities
- The analysis of data pertaining to the bank's activities should consider the following factors:
  - Purpose of the account
  - Actual or anticipated activity
  - Nature of the customer's business
  - Customer's location
  - Types of products and services used by the customer

# Managing Your Risks

## *B. BSA/AML Risk Assessment*

### *1. Risk-Based Approach: Understanding Your Risks*

## **2. Analysis Stage – Cont'd**

### Helpful Reminders:

- No single indicator is necessarily determinative of the risk
- Some risk factors should be weighed more heavily than others
- Conclusion regarding the risk profile should be based on a composite of multiple factors
- Neither define nor treat all members of a specific category of customers as posing the same level of risk

# Managing Your Risks

## *C. Executing AML Requirements*

### 1. Customer Identification Program ("CIP")

- ◆ CIP is part of the bank's overall risk-based AML compliance program
- ◆ A risk-based CIP program requires at a minimum the following:
  - Identify customer for all new accounts
  - Verify the customer's identity
  - Keep records of identifying information
  - Consult sanctions lists
  - Provide notice to customers

# Managing Your Risks

## *C. Executing AML Requirements*

### 2. Elements of Customer Due Diligence (“CDD”)

- ◆ Due diligence conducted by a bank to reasonably believe that it knows its customers
- ◆ An ongoing process designed to:
  1. Verify customer’s identity
  2. Understand customer’s business activities
  3. Anticipate “usual” account/transactional activity
  4. Conduct ongoing transaction monitoring and understanding customer activity

**The majority of customers do *not* pose a risk of illicit activity**

# Managing Your Risks

## *C. Executing AML Requirements*

### 3. Enhanced Due Diligence (“EDD”)

- ◆ EDD is a more comprehensive form of CDD
- ◆ Accounts for which EDD should be conducted include:
  - Foreign Correspondent Banking
  - International Private Banking
  - E-Banking
  - Politically Exposed Persons (“PEPs”)
- ◆ EDD requires additional documentary and non-documentary verification

**EDD is not meant to prevent you from  
doing business**

# Managing Your Risks

## *C. Executing AML Requirements*

### 4. Monitoring and Reporting

- ◆ Suspicious activity reporting is the cornerstone of the BSA reporting system.
- ◆ To identify unusual or potentially suspicious activity, a financial institution will either utilize:
  - Manual transaction monitoring;
  - Automated account monitoring; or
  - A combination thereof.
- ◆ All employees should be responsible for reporting potentially suspicious activity
- ◆ An effective Transaction Monitoring program also assesses the BSA/AML risks at the account opening stage via the completion of a formal risk assessment, which results in a customer risk rating. This resulting risk rating governs the type and degree of transaction monitoring at the inception of the customer relationship.

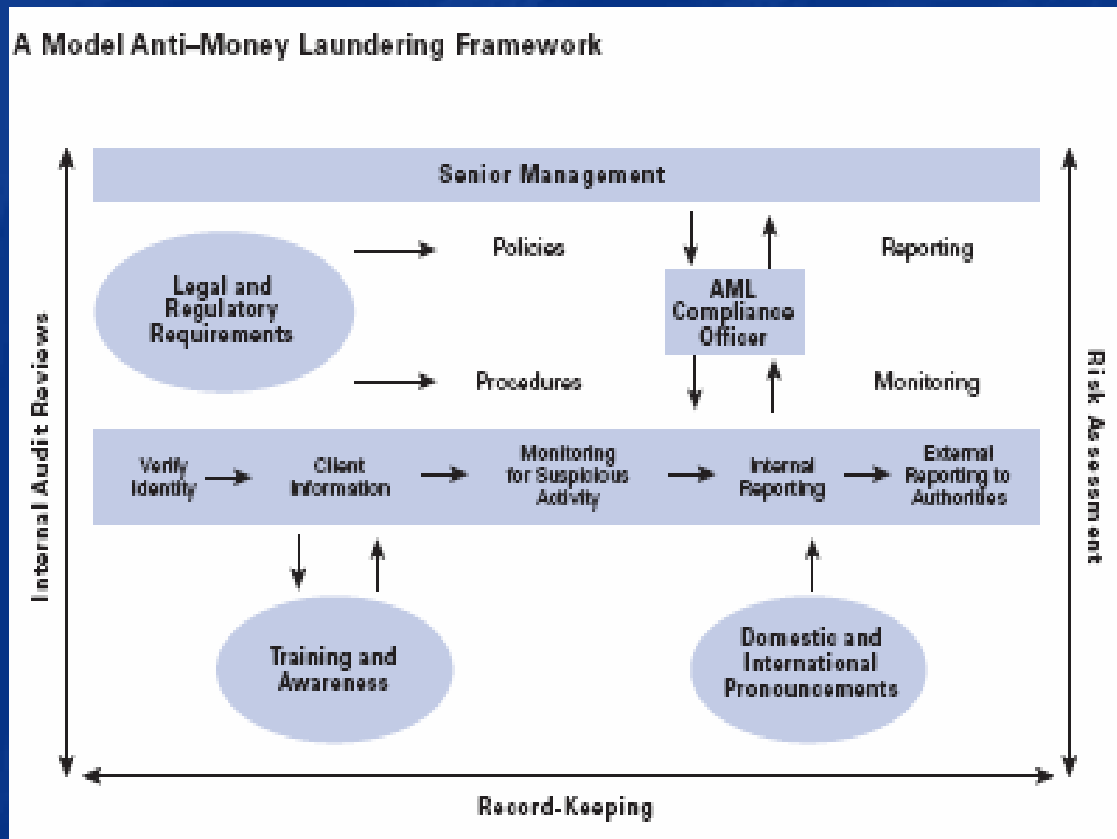
# AML Framework

Senior management set the tone and focus of a bank's risk-based compliance program in three key areas, which together provide the overarching control framework:

1. Setting the bank's policies and procedures
2. Delegating responsibilities through a clear and logical structure
3. Formal monitoring of the operation of processes and internal controls via:
  - Provision of adequate training and awareness to employees
  - A system for testing and verifying the integrity and effectiveness of internal controls across the organization by ensuring for independent testing of BSA/AML compliance program
  - Establishment of appropriate management information system (MIS) statistics on the business and internal controls

# AML Framework – Cont'd

The graph on this slide depicts this overarching control framework visually:



# AML Framework – Cont'd

## ◆ Updating of the BSA/AML Risk Assessment:

- An effective BSA/AML risk assessment is an ongoing process, not a one-time exercise
- Banks should periodically reassess their BSA/AML risks at least every 12 to 18 months
- Management should update the bank's BSA/AML risk assessment to identify changes in the bank's risk profile when:
  - Existing products or services change
  - New products or services are introduced
  - High risk customers open and close accounts
  - Bank expands through mergers and acquisitions

# AML Framework – Cont'd

## ◆ Management's Responsibilities:

- Obtain a comprehensive understanding of the bank's BSA/AML risk exposure and develop appropriate policies, procedures, and processes for monitoring and controlling risk
- Assign explicit responsibility within the bank for ensuring that policies and procedures are managed effectively
- Regularly update policies and procedures, risk assessment, and processes to reflect recent legislative pronouncements and international developments
- For banks that assume a higher risk BSA/AML profile, provide a more robust program to control the risk
- Review the bank's risk assessment for reasonableness during independent testing (internal audit)
- Identify areas with higher risks to better allocate scarce internal audit resources
- A risk or deficiency in one business area may indicate concerns elsewhere in the organization, which management should identify and control
- Implement a robust process of information sharing between the head office, branches, and subsidiaries regarding accounts and activity that may represent heightened risk

# Enterprise-Wide Risk Assessment

## ◆ Financial Holding Companies (FHCs)

- FHCs implementing a BSA/AML risk assessment program should assess both risk individually within the business lines and on a consolidated basis across all activities and legal entities
  - Seek a consolidated understanding of the group's exposure to money laundering and terrorist financing activities
  - Develop group-wide written, comprehensive policies and procedures that capture all aspects of AML within one document
  - Design and implement minimum group-wide AML procedures, supplemented by specific procedures for particular business units and legal entities, where warranted
- Have system and processes in place to monitor and share information across the entire group

# ***Workshop Exercise***

## **BSA/AML Brainstorming Session**

# BSA/AML Brainstorming Session

- ◆ Break out into small groups

- ◆ For each group:

- Assign a scribe
- Using the risk-ranking template, select three examples from each of the following categories:
  - Customers
  - Products and services
  - Geographic locations
  - Transactional activities
- Identify the types of money laundering and terrorist financing risks associated with the examples selected from each category
- Determine the inherent and residual risk rating for each example selected

# Workshop Exercise

From the template provided, select three example from each of the following categories and determine the BSA/AML risks associated with each as well as any mitigating controls around the related processes:

#	Category	Inherent Risk	Rationale/Justification/Internal Controls	Residual Risk
1	Products & Services			
2	Customers & Entities			
3	Geographic Locations			
4	Transactional Activity			

# Workshop Exercise – Example 1

Category	Inherent Risk	Rationale/Justification/ Internal Controls	Residual Risk
<p><b>Products and Services:</b></p> <p><b>Funds Transfers (i.e., Wires)</b></p>	<p><b>High</b></p> <p>High volume of funds transfers to multiple domestic and international jurisdictions on a daily basis</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Analysis reveals that 90% of the wires are recurring transactions for long-term customers.</li> <li><input type="checkbox"/> 70% of the transactions are domestic wires.</li> <li><input type="checkbox"/> All transactions are well-documented by the bank.</li> <li><input type="checkbox"/> Risk is mitigated by well-designed and properly implemented internal controls.</li> </ul>	<p><b>Medium</b></p>

# Workshop Exercise – Example 1: - *A Closer Look at Funds Transfers*

## Advantages for criminal use?

- ◆ Funds transfers (or wires) are the preferred means of transferring illicit funds through the financial system due to the following:
  - Instant
  - Low cost
  - Detection is remote
  - Transfer to jurisdictions that facilitate secrecy or have weak regulations
  - Easy to aggregate funds
  - Movement between accounts to cover up original source

# Workshop Exercise – Example 2

Category	Inherent Risk	Rationale/Justification/ Internal Controls	Residual Risk
<p data-bbox="91 462 325 544"><b>Products &amp; Services:</b></p> <p data-bbox="91 615 405 743"><b>International Correspondent Banking</b></p>	<p data-bbox="458 462 559 501"><b>High</b></p> <p data-bbox="458 625 849 791">A foreign correspondent bank may turn out to be a shell bank.</p> <p data-bbox="458 865 830 1210">The bank may not know with certainty who the correspondent banks' customers are ("Know Your Customer's Customers").</p>	<ul style="list-style-type: none"> <li data-bbox="891 462 1492 629">❑ The bank obtains proper certifications from the foreign bank before a correspondent account is established.</li> <li data-bbox="891 658 1511 782">❑ The bank carefully reviews the certifications for accuracy and reasonableness.</li> <li data-bbox="891 811 1563 1068">❑ The bank mitigates the risks surrounding their correspondent banking relationships as much as possible by closely monitoring transactional activity on these accounts.</li> <li data-bbox="891 1096 1572 1220">❑ The bank conducts Enhanced Due Diligence ("EDD") for all foreign correspondent accounts</li> </ul>	<p data-bbox="1626 462 1797 501"><b>Medium</b></p>

# Sharing of Results

- ◆ Discuss proposed responses or any possible enhancements to the response to each identified risk
- ◆ Discuss any additional issues raised
- ◆ Address possible related regulatory expectations
  - Documentation of the BSA/AML risk assessment process, including the rationale for the determined risk levels
  - Updates to the BSA/AML risk assessment process, as necessary, or at a minimum every 12 to 18 months

***The End***

**Thank you for attending  
the Pre-Conference  
Workshop**