AML- Risk assessment & RBA

EARLEEN MOULTON

VP COMPLIANCE, BRIDGEFORCE FINANCIAL GROUP

Agenda

- What we'll cover and what we won't
- Background on RBA
- Working through it

What is Money Laundering?

- Any effort to **disguise the source** of money or assets derived from criminal activity.
- The act of transforming dirty money into clean money.
- Concealing or converting property or proceeds, knowing or believing the property was derived from committing an offense.

- Money laundering is a prolonged and complicated ***process.*** **Insurance products get used near the end of the process, when cash has already entered the banking system, been converted and has been through a few wash cycles.**

What rules apply to you?

Mandatory Compliance Regime – you must adopt a compliance program and ensure that your employees and those who act on your behalf comply with the Act.

Advisors do not act on behalf of the MGA. Some insurers make compliance program templates available for you to use. See also Advocis and IFB.

Mandatory Compliance Regime

1. Appointment of Compliance Officer
2. Development, application and maintenance of up-to-date written policies and procedures.
3. Documented risk assessment
4. Ongoing training program for staff
5. Regular review of policies and procedures (at least every 2 years) – “self assessment”

Mandatory Compliance Regime

1. Appointment of Compliance Officer
2. Development, application and maintenance of up-to-date written policies and procedures.
3. Documented risk assessment
4. Ongoing training program for staff
5. Regular review of policies and procedures (at least every 2 years) – “self assessment”

Expectation

"FINTRAC expects a well-developed, documented and justifiable RBA process that appropriately identifies, rates, and mitigates the risks to a given entity."

This isn’t new

Customer risk assessment

You must look at every piece of business to determine whether a customer poses a risk.

When you are looking at an application or change form and determining whether it is in “good order, “ also review product type and all relevant information about the customer.

Risk Assessment

You are required to do a risk assessment at least every two years and client risk assessments for each new client.

Risk assessments should take into account

- Product risk
- Channel risk
- Client risk
- Supplier risk
- Geographic risk
- Other risk

Section 3 - Risk assessment

MONEY LAUNDERING/TERRORISM FINANCING RISK ASSESSMENT
(Completed/revised on in accordance with FINTRAC's Guideline 4)

I/We must go through the exercise of analyzing clientele both within business relationships (as defined in legislation) and outside of them, products and services to evaluate my/our own risk based on my/our specific business model. A review of this analysis is conducted every two years and is considered with new clients outside my/our established clientele profile or changes to current client circumstance.

Clientele profile	Yes	No	N/A	Risk Assessment L = Low M = Moderate H = High	Risk-mitigation steps
Description of clientele					
Are any clients:					
-Politically exposed foreign persons?					
-Beneficial owners (non-individual clients: partnerships, associations, businesses, non-profit organization, trusts etc.)?					

Guidance on the Risk-Based Approach to Combatting Money laundering and Terrorist Financing

May 30th, 2015

Explanations/definitions

What is risk?

-the likelihood of an event and its consequences.

-can be seen as a combination of the chance that something may happen and the degree of damage or loss that may result from such an occurrence.

At the reporting entity level

Risks = threats and vulnerabilities that put the reporting entity at risk of being used to facilitate ML/TF.

Threats: could be a person (or group), object that could cause harm. In the ML/TF context, a threat could be criminals, facilitators, their funds or even terrorist groups.

Vulnerabilities: elements of a business that could be exploited by the identified threat. In the ML/TF context, vulnerabilities could be weak controls within a reporting entity, offering high risk products or services, etc.

Impact: refers to the seriousness of the damage that would occur if the ML/TF risk materializes (i.e. threats and vulnerabilities)

What is risk management?

- a process widely used in the public and private sector to assist in decision-making.

When dealing with ML/TF, it's the process that includes:

- the recognition of ML/TF risks,
- the assessment of these risks, and
- the development of methods to manage and mitigate the risks identified.

What are inherent & residual risks?

Inherent risk is the intrinsic risk of an event or circumstance that exists before the application of controls or mitigation measures.

Residual risk is the level of risk that remains after the implementation of mitigation measures and controls.

Important to note - the risk assessment exercise described in this document focuses on the inherent risks to your business, activities and clients.

What is a risk-based approach(RBA)?

The **risk assessment** of your business activities and clients using certain prescribed elements;

- Products, services and delivery channels;
- Geography;
- Clients and business relationships, and
- Other relevant factors.

- The **mitigation of risk** through the implementation of controls and measures tailored to the identified risks;
- Keeping **client identification** and, if required, beneficial ownership and business relationship information up to date relative to the assessed level of risk; and
- The **ongoing monitoring** of transactions and business relationships in accordance with the assessed level of risk.

This is not a static exercise

- Assessing and mitigating risk is a step by step process, and cyclical.
- Risks assessed may change/evolve over time.
- Your RBA must be re-evaluated and updated when the risk factors change

Risk-based approach cycle

1. Identification of your inherent risks (business-based risk assessment along with the relationship-based risk assessment)
2. Setting your risk tolerance
3. Creating risk-reduction measures and key controls
4. Evaluating your residual risks
5. Implementing your risk-based approach
6. Reviewing your risk-based approach.

Step 1 - Identify inherent risks

Business-based risks:

- Products, services, delivery channels
- Geography
- Other relevant factors

Assess the risk in your business activities

- **Take a business-wide perspective**. This will allow you to consider where risks occur across business lines, clientele or particular products
- **Look at your vulnerabilities** to ML/TF
- Areas identified as **high-risk will require documented mitigation** strategies
- The actual number of **risks in your inventory will vary** based on the type of business activity you conduct and products and services you offer

Products

If product sold is non-registered

- UL/whole life
- segregated fund
- endowment or annuity or
- any plan with a lump sum payment of $100,000 or more,

Consider these higher risk.

Why are insurance products attractive?

- Lots of investment options
- Liquidity
- Portability and ease of transfer
- Can purchase in large amounts without triggering a regulatory inquiry
- Insurance changes the form of the funds
- Sometimes money launderers use dirty money to buy insurance because they need insurance like the rest of us

High risk business practices

Do you conduct non face-to-face sales?

Do you take cash and/or money orders?

Do you deal with corporations, trusts, foundations/charities?

Do you deal with lawyers, accountants POA or others acting for the client?

Do you deal with third parties?

Are your clients PEPs(foreign or domestic)?

Geography

- Border-crossings, especially with other countries
- Rural/urban setting
- Located in known high crime-rate areas
- Connection to high-risk countries
  - Special Economic Measures Act (SEMA)
  - Financial Action Task Force (FATF) list of High-Risk Countries and Non-Cooperative Jurisdictions
  - Freezing Assets of Corrupt Foreign Officials Act Sanctions (FACFOA)

Other relevant factors

Business model:

- Size of your business
- Number of locations/branches, number of employees and/or subagents
- Turnover of staff
- Use of service providers, especially where they may be checking client ID

Documenting your assessment

A couple of options:

- Simple, bullet-form notation
- Enhance your existing risk assessment
- Consider the following …

Section 3 - Risk assessment

MONEY LAUNDERING/TERRORISM FINANCING RISK ASSESSMENT
(Completed/revised on in accordance with FINTRAC's Guideline 4)

I/We must go through the exercise of analyzing clientele both within business relationships (as defined in legislation) and outside of them, products and services to evaluate my/our own risk based on my/our specific business model. A review of this analysis is conducted every two years and is considered with new clients outside my/our established clientele profile or changes to current client circumstance.

Clientele profile	Yes	No	N/A	Risk Assessment L = Low M = Moderate H = High	Risk-mitigation steps
Description of clientele					
Are any clients:					
-Politically exposed foreign persons?					
-Beneficial owners (non-individual clients: partnerships, associations, businesses, non-profit organization, trusts etc.)?					

Column A: **LIST OF FACTORS** *Identify all the factors that apply to your business (i.e. products, services and delivery channels, geography, other relevant factors*	Column B: **RISK RATING** *Assess each factor (e.g. low, medium or high)*	Column C: **RATIONALE** *Explain why you assigned that particular rating.*	Column D: **DESCRIBE MITIGATION MEASURES FOR HIGH RISKS IDENTIFIED IN COLUMN A.**

Scoring your assessment

All inherent risks identified need to be given a risk level

The scale should be tailored to the size and type of business, for example:

- Advisor (sole proprietor) engaged in traditional practice could use L and H risk
- Agency with staff, sub-agents, multiple locations - e.g. medium, medium-high, high

The law requires you:

Every risk element identified as “high-risk” must be addressed with mitigation measures and be documented.

You will have to be able to demonstrate to FINTRAC that controls/measures have been put in place to address these high-risk elements (e.g. in your policies and procedures, training program) and that they are effective (through your internal or independent review).

Non-face-to-face delivery channels (telephone, online, mobile)	High risk	Potential third party involvement in the payment or receipt of products.	• Increase employee awareness of the risk of online markets. • Identify and verify customers before entering into a business relationship. • Set parameters within which certain transactions require management review and approval.
Proximity to a large border crossing with USA	High risk	Business may be the first point of entry into the financial system.	• Increase employee awareness through training so that staff better understand the placement stage of money laundering and its potential impacts. • Attempt to obtain information to understand the customer's circumstances / business. • Put a limit on cash transactions.

Step 1 (B) - Identify inherent risks

Relationship-based risks -

Advisors encounter specific and direct ML/TF risks because of the nature and type of business that your clientele has with you through:

- Products, services and delivery channels they utilize
- Their geography
- Characteristics and patterns of activity

Examples of high risk clients/transactions

- Behaviour or transactions that are unusual compared to other similar clients.
- A client's business is cash intensive or generates cash for transactions not normally cash intensive
- A client's business structure makes it difficult to identify its true owners or controllers
- An individual with a high-level position, influence and/or connections (Politically Exposed Foreign Persons)
- A client has ties to or conducts business in a high-risk country
- A client transactions are non-face-to-face

More examples

- Does owner's or payor's occupation generate a lot of cash, if known? (i.e. variety stores, pizzerias, money service businesses, etc). Cash businesses are higher risk than others.
- Does the customer have ties to any countries that:
  - have weak AML-ATF laws or are not FATF members
  - Appear in the Special Economic Measures Act Regulations (http://laws-lois.justice.gc.ca/eng/acts/S-14.5/)
  - Appear on the OSFI List of Designated names? http://www.osfi-bsif.gc.ca/Eng/fi-if/amlc-clrpc/atf-fat/Pages/default.aspx.

You are required to pay attention to this and check these sites. If you believe you have a name match, do not continue with the transaction. Contact BFG or insurer.

Where do most clients fall?

Most advisors will only have one or two client risk groupings.

If you identify high-risk clients or groups – what's the predominant reason for most to be classified as high-risk?

Scoring your assessment

All inherent risks need to be given a risk level

The scale should be tailored to the size and type of business, for example:

- Advisor (sole proprietor) engaged in traditional practice could use L and H risk
- Agency with staff, sub-agents, multiple locations - e.g. medium, medium-high, high

Documenting your assessment

If you can, keep it simple, bullet-form notation

For example: “I’ve identified no high-risk client relationships in my business. My relationship-based risk is low because transactions are low to medium in value, conducted face-to-face and transactions are in line with the client’s profile”

If you have multiple risk-groupings, your documentation should be tailored to your risk.

Column A: **BUSINESS RELATIONSHIPS** *Identify all your business relationships or high-risk clients (individually or as groupings)*	Column B: **RISK RATING** *Assess each business relationship (e.g. low, medium or high)*	Column C: **RATIONALE** *Explain why you assigned that particular rating*	

Step 2 – Set your risk tolerance

Set risk tolerance you are willing to accept. Risk categories to consider:

- Regulatory risk
- Reputation risk
- Legal risk
- Financial risk

Must be taken into account before moving on to consider *how* risks can be addressed. Risk tolerance has direct impact on Step 3, policies and procedures, and your training plan.

Ask yourself:

- Are you willing to accept regulatory, reputational, legal or financial risks?
- What risks are you willing to accept only after implementing some mitigation measures?
- What risks are you not willing to accept?

Your obligation

The PCMLTF Act and Regulations state that you/your organization has mandatory obligations in situations where high-risk business activities and high-risk business relationships are identified.

This step does not allow reporting entities to avoid these obligations.

Step 3 – Risk reduction measures and key controls

- As part of your compliance program, you must develop and document risk mitigation strategies
- This serves to limit the ML/TF risks you've identified during the risk assessment
- Allows you/your business to stay within the risk tolerance you've set.

Expectations

For **all situation and all clients**:

- Internal controls to mitigate overall risks (training, servicing clients, keep your compliance program up to date)
- Conduct on-going monitoring, keep a record of what and how

For **high-risk** business and client relationships:

- Document measures to mitigate risk
- Conduct more frequent monitoring of high-risk relationships
- Enhance measures to ascertain ID, keep client information up to date

Specifics?

For **detailed** information on risk mitigation measures, consult sections 6.2, 6.3 and 6.4 of *Guideline 4: Implementation of a Compliance Regime*.

Ensure you're keeping records on the information obtained on product applications.

Column A: **LIST OF FACTORS** *Identify all the factors that apply to your business (i.e. products, services and delivery channels, geography, other relevant factors*	Column B: **RISK RATING** *Assess each factor (e.g. low, medium or high)*	Column C: **RATIONALE** *Explain why you assigned that particular rating.*	Column D: **DESCRIBE MITIGATION MEASURES FOR HIGH RISKS IDENTIFIED IN COLUMN A.**

Non-face-to-face delivery channels (telephone, online, mobile)	High risk	Potential third party involvement in the payment or receipt of products.	• Increase employee awareness of the risk of online markets. • Identify and verify customers before entering into a business relationship. • Set parameters within which certain transactions require management review and approval.
Proximity to a large border crossing with USA	High risk	Business may be the first point of entry into the financial system.	• Increase employee awareness through training so that staff better understand the placement stage of money laundering and its potential impacts. • Attempt to obtain information to understand the customer's circumstances / business. • Put a limit on cash transactions.

Column A: **BUSINESS RELATIONSHIPS** *Identify all your business relationships or high-risk clients (individually or as groupings)*	Column B: **RISK RATING** *Assess each business relationship (e.g. low, medium or high)*	Column C: **RATIONALE** *Explain why you assigned that particular rating*	

Column D:	Column E:	Column F	Column G:
DESCRIBE ENHANCED MEASURES TO ASCERTAIN ID FOR HIGH-RISK BUSINESS RELATIONSHIPS	DESCRIBE MITIGATION MEASURES FOR HIGH-RISK BUSINESS RELATIONSHIPS	DESCRIBE PROCESS TO KEEP CLIENT INFORMATION UP TO DATE FOR HIGH-RISK BUSINESS RELATIONSHIPS	DESCRIBE ENHANCED ONGOING MONITORING FOR HIGH-RISK BUSINESS RELATIONSHIPS

Column A: **BUSINESS RELATIONSHIPS** *Identify all your business relationships or high-risk clients (individually or as groupings)*	**Column B:** **RISK RATING** *Assess each business relationship (e.g. low, medium or high)*	**Column C:** **RATIONALE** *Explain why you assigned that particular rating*	**Column D:** **DESCRIBE ENHANCED MEASURES TO ASCERTAIN ID FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Column E:** **DESCRIBE MITIGATION MEASURES FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Column F** **DESCRIBE PROCESS TO KEEP CLIENT INFORMATION UP TO DATE FOR HIGH-RISK BUSINESS RELATIONSHIPS**	**Column G:** **DESCRIBE ENHANCED ONGOING MONITORING FOR HIGH-RISK BUSINESS RELATIONSHIPS**
• Group A	Low	Medium value transactions conducted face-to-face in line with the client's profile.	**N/A**	**N/A**	**N/A**	**N/A**

• Politically Exposed (Foreign) Person (PEP or PEFP))	High	A PEP/PEFP is an individual who may be vulnerable to ML/TF or corruption due to their position, relationships or influence.	Implement training programs to ensure employees can identify PEP /PEFP clients and to understand, assess and handle the potential associated risks.	Require senior management approval to open new accounts or maintain existing accounts. Set transaction thresholds (dollar value and/or frequency) and request information on the source of funds for transactions above thresholds.	Ask client to confirm or update their identification information at every threshold transaction.	Obtain additional information about the client's source of funds or the client's source of wealth. Increase the monitoring of transactions of higher-risk products, services and channels. Identify patterns of transactions that require further examination.

• Clients for whom Suspicious Transaction Reports (STR) have been previously submitted	High	Reasonable grounds for suspicion have already been established through submission of STRs.	Make thresholds for ascertaining identification more stringent for clients with similar characteristics.	Set threshold and request information on source/destination of funds for any amounts above threshold.	Ask client to confirm or update their identification information at every threshold transaction.	Review transactions conducted by client more frequently. Identify patterns of transactions that require further examination.

Step 4 – Evaluate your Residual Risks

- The remaining level of risk after taking into account the mitigation measures and controls
- Even with all measures and controls in place, there will be some residual exposure to manage.

Tolerated risks: They're still risks, and may increase over time.

Mitigated risks: Although lessened/reduced, they're still risks. Measures to mitigate could fail, not be followed, etc.

Step 5 – Implement RBA

- Implement your risk mitigation measures and controls as part of your day to day activities.

- Apply or put into practice, the risk-reduction strategies and key control for high-risk (ML and TF) situations.

Step 6 – Review your RBA

- Review or test your risk-based assessment for effectiveness.
- Minimum every 24 months, more often if there are material changes
- Make changes or adjust as necessary

Questions?