Detailed Briefing: The Risk-Based Approach to Customer Due Diligence (CDD) and AML/CFT Frameworks

Executive Summary

This briefing outlines the critical role of a Risk-Based Approach (RBA) in Anti-Money Laundering (AML) and Counter-Terrorist Financing (CFT) frameworks, with a particular focus on Customer Due Diligence (CDD). The RBA, mandated by FATF, optimises resource allocation by applying varying degrees of scrutiny based on identified money laundering (ML) and terrorist financing (TF) risks. It covers the identification of risk factors, the assignment of risk ratings, the application of tailored CDD measures (Simplified, Standard, Enhanced), and the importance of firm-wide risk assessments and risk acceptance processes. The document also highlights the consequences of inadequate AML/CFT controls, including regulatory penalties and reputational damage.

Key Themes and Most Important Ideas/Facts

1. The Risk-Based Approach (RBA) to AML/CFT

- **Core Principle:** The RBA involves "applying a higher degree of scrutiny to areas where risks are higher, hence optimising the way resources are allocated to combat money laundering and terrorism financing." It is mandated by FATF Recommendation 1 and forms the "cornerstone of present-day requirements in AML/CFT."
- **Application:** The RBA is applied at three levels:
  - Countries: Governments perform 'National Risk Assessments' to evaluate vulnerabilities and formulate action plans.
  - Regulated Entities (Firm-Wide): Firms assess and manage risks across their businesses and customers.
  - Customer Relationships: Firms tailor CDD measures to individual customers based on their assessed ML/TF risk. This briefing focuses primarily on customer relationships.
  - Importance of RBA:Flexibility: It allows countries and institutions to "adopt a more flexible set of measures, in order to target their resources more effectively and apply preventive measures that are commensurate to the nature of risks."
  - Resource Allocation: Enables the allocation of "limited resources... to the areas where higher levels of risk have been identified."
  - Tailored Measures: Ensures AML/CFT measures are "sufficiently robust but at the same time do not create excessive demands."

2. Customer Due Diligence (CDD) and its Dynamic Nature

- **Purpose:** CDD is a continuous process applied at each stage of the customer relationship to understand the customer, the true origins of their funds, and ensure legitimate business activities. It also includes "other related AML/CFT activities relating to sanctions, PEPs, suspicious activity and law enforcement enquiries, and prevent fraud."

- **Dynamic Process**: CDD is "dynamic and iterative." An initial low-risk assessment can change to medium-risk due to evolving circumstances, prompting further enquiries and a new risk rating.
- **Offboarding:** When offboarding a customer, a firm must:

1. Identify all accounts across the firm.
2. Have appropriate commercial and legal communications.
3. Manage outstanding transactions.
4. Properly close accounts.
5. Update CDD records.
6. Ensure no new business is undertaken.

3. Key Risk Factors and AML 'Red Flags'

Firms identify risk factors based on information collected about the customer, beneficial owners, and the nature of the relationship. Common risk factors include:

- Entity Risk: Higher risk for entities that conceal identity (trusts, shell companies, bearer shares); lower risk for publicly listed or regulated entities.
- Country Risk: Varies based on robustness of AML/CFT regimes, crime levels, corruption, and support for terrorism. Firms use internal analysis and external reports (e.g., FATF reviews, Transparency International's Corruption Perceptions Index).
- Business Risk: Certain activities are vulnerable to money laundering (e.g., cash-intensive businesses, MSBs, gambling, real estate, luxury goods).
- Product Risk: Products/services more vulnerable to ML (e.g., correspondent banking, trade finance, private banking) or inconsistent with business activities.
- Delivery Channel Risk: Mechanisms that carry inherent ML risks (e.g., non-face-to-face relationships, use of distributors).
- Sanctions Risk: Risk of doing business with sanctioned individuals/organisations or in sanctioned countries. Requires "systematic screening."
- PEP Risk: Politically Exposed Persons (PEPs) require Enhanced Due Diligence (EDD) due to higher exposure to bribery/corruption and reputational risk.
- Reputational Risk: Broader risk arising from customer profile or activities (e.g., financial difficulties, conduct issues, regulatory enforcement, social/environmental issues). Detected via "adverse media reports."
- AML 'Red Flags': Behavioural indicators of possible money laundering, often sector-specific. Examples include:

➢ "reluctance to provide CDD information, including vague or incomplete answers"
➢ "applying pressure to open the account quickly"
➢ "unusual willingness to provide information" or "unusual knowledge of the firm's CDD procedures"
➢ "convoluted or unclear description of business activities or of the purpose of the relationship"
➢ "transaction does not appear to have a clear economic purpose"
➢ "corporate customer exhibits overly complex ownership structures"
➢ "documentation provided is unclear or unprofessional"

- Unusual Activity: Detected through "ongoing monitoring," includes "Transactions which are substantially larger in value than usual," "substantially more complex than usual," or "does not correspond to the regular pattern."

4. Applying Simplified, Standard, and Enhanced Due Diligence (SDD, CDD, EDD)

The RBA dictates different levels of CDD based on risk:

- **Simplified Due Diligence (SDD):** Applied to low-risk customers, primarily focusing on "customer identification element of CDD." Enquiries are limited, beneficial owners may not be assessed or only if ownership exceeds 25%, purpose assessed at a high level, and future reviews less intensive. "SDD is therefore not an exemption to carry out CDD checks and should never be applied when specific risk factors are known to exist."
- **Standard Due Diligence (CDD):** Applied to medium-risk customers. Involves "collecting a broader range of information about the customer, its beneficial owners and the purpose of the relationship." Requires "Independent verification of information from the customer."
- **Enhanced Due Diligence (EDD):** Applied to high-risk relationships. It is a "key requirement" and "mandatory regulatory obligation in certain situations, such as relationships with PEPs or correspondent banks." EDD measures include:

➔ Verification of customer information using "sources independent from the customer including, where necessary, certification by third parties or the use of more than one source of information."
➔ Detailed investigation and independent verification of business activities, potentially "including on-site visits."
➔ Detailed establishment and verification of the customer's "source of wealth."
➔ Closer scrutiny of ownership structure, using "lower beneficial ownership threshold – commonly 10% – rather than the 25% common in standard CDD."
➔ "reputation checks on beneficial owners and controllers (an adverse media check)."
➔ More detailed documentation of the relationship's purpose, including "assessment of the source of funds... externally verified to a degree."
➔ More granular assessment of expected activity levels for monitoring.

5. Risk Rating and Acceptance

- **Risk Rating:** Risk factors are aggregated to create a risk rating (low, medium, high). Firms use "risk rating methodology to measure the risks... in a standardised manner," applying a model to identified risk factors. A simple model like BestCredit's demonstrates how even one "higher-risk factor" can designate a customer as high-risk.
- **Risk Acceptance:** The process of validating the acceptability of a customer relationship. It comprises three components:
- Risk Assessment: "Assessment of the risks posed by the customer relationship, based on the risk factors identified and the risk rating assigned." This involves a written analysis and results in a "customer risk profile."
- **Risk Mitigation:** "Measures to counteract the risks of the relationship; these measures will constitute the conditions attached to the relationship." Examples include "restricting the products and services available," "applying a higher intensity of transaction monitoring," "increasing the frequency of periodic reviews," and

"quarantine of payments." These measures allow firms to accept relationships they might otherwise decline.

- **Risk Approval:** "A formal process of approval of the relationship under the agreed conditions." This involves documenting the assessment and mitigation, allocating responsibilities, and ensuring clear ownership of the risk profile.
- **Exiting Relationships (De-risking)**: If risks fall outside the firm's risk appetite or mitigation costs are too high, a firm "may decide not to onboard the customer at all, or to terminate an existing relationship."

➔ Definition: "De-risking consists in exiting entire segments of customers when the risk profile of the relationships fall outside of the risk appetite of the firm, or when the costs of mitigating measures become commercially unviable."

➔ Impact: Affects high-risk areas like correspondent banking and MSBs, and can lead to "civil claims from customers affected," "adverse media attention," and "reputational risks" (e.g., Dahabshiil and Barclays case).

- **Importance of Risk Acceptance:** It is the "principal outcome of the entire CDD process," demonstrating effective AML/CFT duties, regulatory compliance, evidence of decision-making, and protection against penalties and reputational damage.

6. Firm-Wide Risk Assessments

- **Foundation:** A "key regulatory expectation and the foundation of an effective risk-based approach to AML/CFT."
- **Purpose:** To "identify and evaluate the risks to which a firm is exposed." It enables firms to understand their vulnerability to ML/TF and calibrate AML/CFT resources.

➔ Key Disciplines:Identification of Inherent Risks: Understanding risk factors across customer base, industries, products, services, geography, and delivery channels. FATF guidance highlights factors like "The nature, scale, diversity and complexity of their business" and "The jurisdictions the bank is exposed to."

➔ Qualifying Risk Factors: Assessing the severity of risks using guidance material, National Risk Assessments, and country reports.

➔ Management of Firm-Wide Risk: Dynamic process, requiring frequent review and updates (usually "at least once a year").

➔ Outcomes:Meaningful RBA Definition: Based on analysis of inherent risk factors.

➔ Calibration of Systems and Controls: Ensuring consistent application across all activities and jurisdictions.

➔ Risk Appetite Statement (RAS): Articulating "how much risk it is willing to take, given its business model, and the level of controls it is willing or able to apply."

➔ Business Decisions: Informing decisions on entering new markets or developing products based on risk appetite.

- **Documentation:** "Risk assessments should be thoroughly documented" for senior management, regulators, and internal improvements.
- **Systems and Controls:** A "key outcome" is the development of adequate systems and controls, including "governance and senior management ownership," "3LOD," "AML compliance activity," "policies and procedures," "monitoring systems," "management information," and "training."

- **Residual Risk:** The risk that remains after controls have been applied. If above a threshold, firms may "abandon the activity," "seek senior management approval," or "Review and improve the controls."
- **Senior Management Responsibilities:** "Accountable for the firm's management of financial crime risks and the implementation of adequate systems and controls," and for setting a clear risk appetite.

7. Consequences of Failures

The sources provide examples of severe consequences for firms that fail to apply correct AML/CFT procedures, including:

- **Fines and Criminal Liabilities:** "There are severe consequences for firms who breach sanctions, in the form of both fines and criminal liabilities."

➔ Regulatory Penalties:UOB Kay Hian Private Limited in Singapore fined $375,000 for "failure in its AML/CFT controls and business conduct," including falsified CDD information.

➔ HSBC Bank Plc fined £63 million by UK FCA for "serious weaknesses... in the bank's transaction monitoring systems" over an eight-year period.

➔ Citibank, DBS Bank, OCBC Singapore, and Swiss Life (Singapore) received penalties totalling S$3.8 million for "inadequate AML/CFT controls" related to Wirecard AG. Swiss Life's issues included "Insufficient understanding of complex ownership and control structure of a higher-risk customer" and "Inadequate corroboration of the source of wealth for the customer's BO."

- **Reputational Damage:** As seen in the Dahabshiil and Barclays case, where Barclays' de-risking decision "attracted much publicity as aid groups criticised" it, leading to "collateral challenges of increasing AML/CFT regulations."

This detailed briefing underscores that a robust and dynamic risk-based approach to CDD, supported by comprehensive firm-wide risk assessments and strong senior management oversight, is essential for effective AML/CFT compliance and to mitigate financial, regulatory, and reputational risks.