Deloitte.

Emerging trends and solutions in AML/CFT

Radish Singh, Southeast Asia Anti-Money Laundering & Sanctions Leader

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Key recent regulatory developments: Global (1 of 2)

The Fourth EU AML Directive

- Enacted in early 2015; The directive needs to be built into national laws by EU states by June 26 2017.
- Some of the key changes from the previous directive are:
  - **Risk Assessments**: EU states to perform National Risk Assessment to evidence steps to manage AML/CTF risk
  - **CDD**: Prescribes factors to consider before applying simplified CDD (SCDD) to a customer. Entities to evidence why risk was considered low enough to apply SCDD (in past there was blanket application of SCDD when clients fell in a category)
  - **Beneficial Ownership**: Requirement for legal persons (e.g. companies, Trusts) to hold adequate, accurate, and current information on their own beneficial ownership and provide the same to competent authorities & obliged entities
  - **PEPs**: Definition extended to include domestic PEPs. Risk posed by PEP to be monitored for 18 months (instead of 12 months) when a person ceases to hold title yielding PEP status
  - **Record Keeping**: Retention period for CDD documents after business relationship end to be 5 years. Period can be extended by up to 10 years if local legislation applies
  - **Policies & Procedures:** Provision for consideration of data protection elements within AML/CTF policies for sharing of customer information. Provides clarity to application of AML/CTF rules for subsidiaries in countries where legislation is deemed deficient, or non-equivalent.
  - **Third Party Equivalence**: List of equivalent jurisdictions has been rescinded. Entities will need to perform a risk assessment on each country of business
  - **Definition of Senior Management** not restricted to the Board of Directors

United Kingdom

- **The Fourth EU AML Directive:** Being a EU state, UK needs to comply with the Fourth EU AML Directive. UK Treasury is in the process of reviewing the directive and driving the formulation of legislation
- **SAMLP**: The FCA has been carrying out deep dive assessments of major banks as part of our Systematic Anti-Money Laundering programme (SAMLP). In September 2014, FCA started a new inspection regime for a group of smaller firms which present higher inherent money laundering risk. In 2014/15 six early interventions on AML were carried out
- **JMLIT:** Since April 2014, FCA has played a key role in establishing a mechanism for improved information-sharing between financial institutions and law enforcement organisations. Working in collaboration with the Home Office and the Bank of England, plus a range of banks and other organisations, FCA developed the JMLIT (Joint Money Laundering Intelligence Taskforce), a 12-month pilot project. Its aim is to improve intelligence-sharing arrangements to help fight money laundering and financial crime
- **De-risking**: Guidelines have been issued around de-risking so that banks can strike a balance between not offering financial services to entire categories of customers and managing financial crime risks. FCA published a statement on de-risking on 27 April 2015 to provide guidance to financial institutions
- **Simplification of Laws**: FCA has also been working with financial institutions to simplify the AML/ CFT laws so that it is easier for financial institutions to comply with these regulations. FCA had also initiated a feedback programme from the industry participants

Key recent regulatory developments: Global (2 of 2)

United States

- **Individual accountability**: Regulators have been pushing for personal liability and accountability for individuals for their actions and for compliance-related deficiencies within their areas of responsibility. The government has increased scrutiny of AML compliance officers and their potential personal liability
- **Leadership**: Regulators have sent a strong signal that a robust risk-management framework that is consistent with regulatory expectations will not be enough by itself. To be truly effective, the framework must be reinforced by the proper "tone at the top"
- **De-risking**: Regulators and law enforcement expressed concern that some institutions have been "de-risking" or exiting whole business lines that carry increased risk, instead of improving risk management and controls and evaluating customers individually
- **Emphasis on certain businesses**: Regulators have placed emphasis on relationships with money services businesses (MSBs), third-party payment processors (TPPPs) and correspondent banking relationship with Shell banks
- **CDD**: Amendments proposed by FinCEN to existing BSA regulations around customer due diligence requirements specifically around beneficial ownership requirement
- **Proposed AML Regulations:** New York Department of Financial Services' proposed AML regulations include a personal certification of AML compliance, Random testing of transactions data from financial institutions has also been proposed by the regulators
- **Virtual Currencies**: In 2015, the Conference of State Bank Supervisors issued a model regulatory framework, and at least one state issued final rules for regulating virtual currency firms, each of which includes provisions related to BSA/AML compliance. FinCEN highlighted virtual currency as an ongoing priority (first enforcement action against a virtual currency exchange)

Hong Kong

- **Screening and Transaction Monitoring**: With Hong Kong being a global payments hub, HKMA has emphasised the importance of effective screening and transaction monitoring systems in all AML/CFT supervision. Recent guidance on transaction monitoring has been issued. HKMA highlighted the importance of having automated transaction monitoring systems as well as effective alerts management process. Screening and transaction monitoring will continue to be a focus going forward
- **Risk Assessments**: Emphasis on establishment of AML/CFT comprehensive risk assessment framework. It includes identification and assessment of inherent risks supported by quantitative and quantitative analysis, risk mitigation and ability to update the assessment regularly
- **Governance and Oversight**: Focus on Governance and Oversight of ML/TF risks remain a key focus of supervision. HKMA emphasised that assurance activity should be performed by compliance function over the CDD or sanctions process – to detect control failures. Also, key post holders, MLRO etc., must be effective
- **CDD**: Additional push on performing risk based customer due diligence e.g. application of EDD, extensive due diligence for correspondent banking, identification of source of wealth and identification of PEPs
- **Tax Evasion**: Guidance paper on Anti-Money Laundering controls over tax evasion have also been issued by HKMA

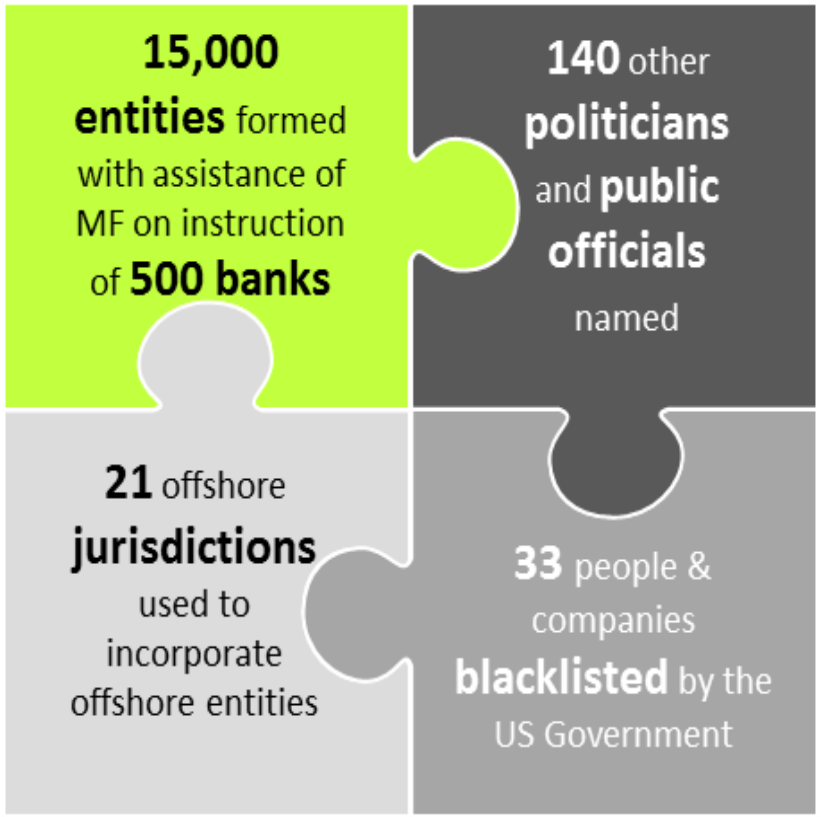
Key recent regulatory developments: Singapore

Some of the key recent regulatory changes and developments in Singapore have been summarised below:

- **Comprehensive Assessment of Risks**: MAS 626 imposes obligations on Banks to identify and assess the overall ML/TF risks they each face as an institution, and to take necessary steps to mitigate such risks. Banks are also required to undertake risk assessments of new products, practices and technologies prior to their launch, to decide whether such launch will lead to ML/TF risks, and to take measures to manage and mitigate such risks
- **Cross-border Wire Transfers Exceeding S$1,500:** MAS 626 states that the Banks are required to perform CDD when effecting or receiving funds by domestic wire transfer/ cross-border wire transfer that exceeds S$1,500 for a customer who has not established business relations with them.
- **Identification and Verification of the Identity of Beneficial Owners**: MAS 626 defines the Banks need to undertake when identifying and verifying the identity of beneficial owners of non-individual customers, such as companies and trusts. When dealing with customers which are companies, Banks are to identify and verify the identity of the natural person who ultimately owns the company. When dealing with customers which are trusts, Banks are to identify and verify the identity of the trustee(s), settlor, protector , beneficiaries, and any natural person exercising ultimate ownership or control over the trust.
- **Customer Screening**: Banks are required to screen their customers, natural persons appointed to act on behalf of their customers, connected parties of their customers and beneficial owners of their customers against relevant ML/TF information sources, as well as lists and information provided by the MAS and any relevant Singapore authorities for the purpose of determining if there are any ML/TF risks.
- **Politically Exposed Persons (“PEPs”):** The MAS has introduced a new category of PEPs, a category of customers considered to be of high risk. In addition to performing CDD measures, Banks are required to perform enhanced CDD on PEPs, their family members and close associates. In addition, Banks are to adopt a risk-based approach, in determining whether to perform enhanced CDD or the extent of enhanced CDD to be performed, for specified categories of PEPs, their family members and close associates
- **Guidance on AML/ CFT in Trade Finance and correspondent banking**: The guidance outlines the detailed controls and measures to prevent ML/CFT risks associated with trade finance and correspondent banking

Recent developments – The Panama Papers

13 April 2016: The EU has plans for large multinationals to report earnings and pay taxes – change necessary due to Panama Papers scandal



Order from the New York Department of Financial Services sent to 13 foreign banks identified in articles published by ICIJ and its media partners. The banks have been given 10 days to respond, and were asked to provide communications, phone logs and records of transactions between their New York branches and employees or agents of Mossack Fonseca, as well as any subsequent communication with shell companies formed as part of these transactions. According to Bloomberg, the regulator has also asked banks to identify any New York-based personnel who may have held positions at the shell companies.

11 April 2016 - Cameron pledged to create a cross agency task force to probe Panama Papers revelations and promised to push for new rules that would allow authorities to prosecute corporations that facilitate tax evasion.

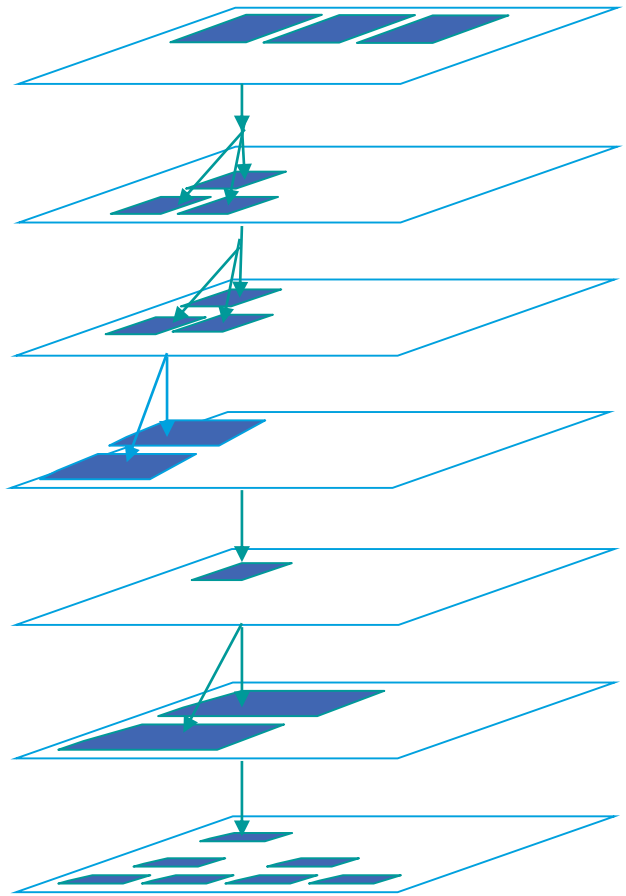
Source: https://panamapapers.icij.org/

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Regulatory change is complex due to impact & rapid expansion of scope

For ensuring effective response to address the regulatory change, the complexities of Financial Crime operating model need to reviewed through various lenses



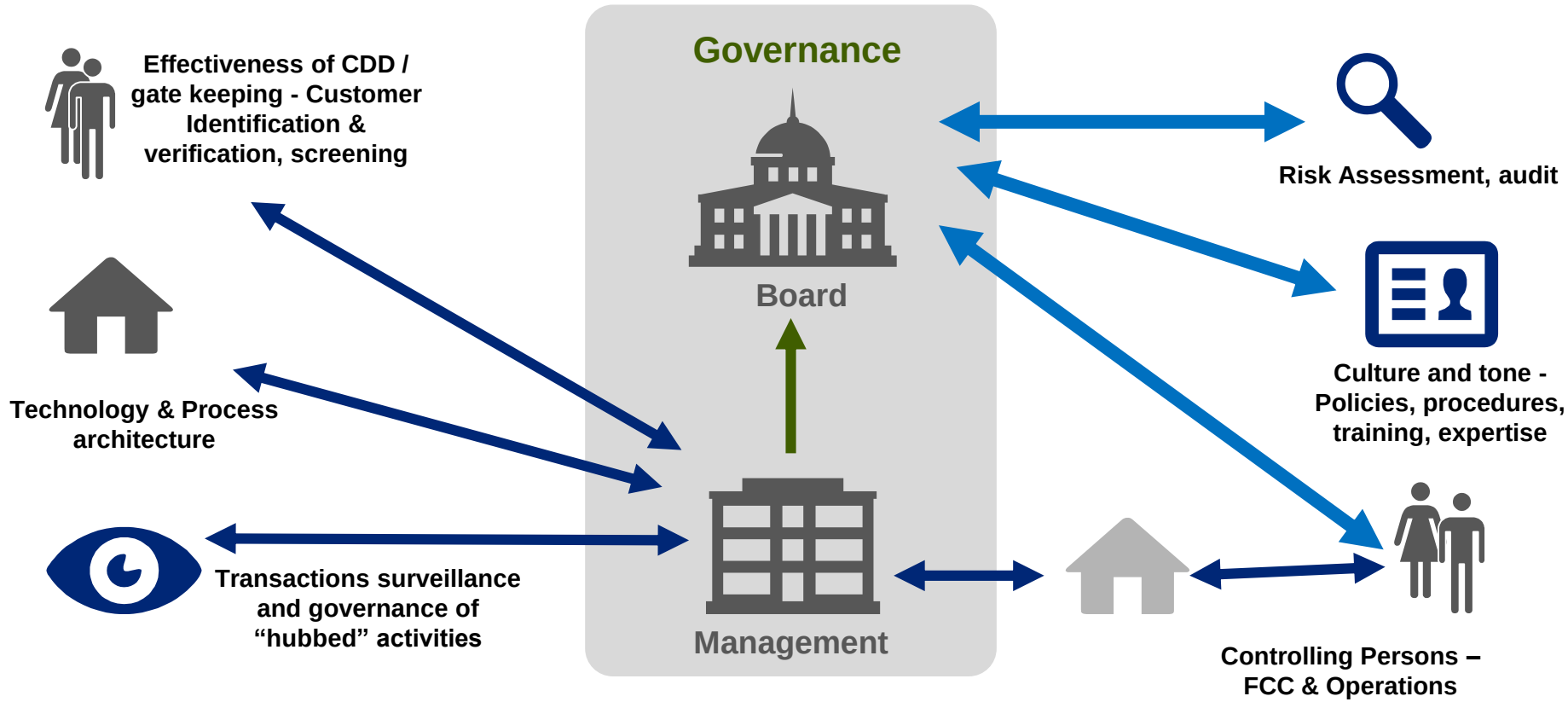
Operating model components	Business questions answered (Representative)	Areas impacted
Clients/ Products	• What impact will the trade finance services have on Financial Crime Risk? • How should I risk rate a Correspondent banking relationship?	• Types of clients currently serviced; Plans for the future • Products currently offered; Future product offerings
Policy	• Can I have standard AML policies across jurisdictions? • What is the level of detail required?	• All policy documents across business lines
Processes	• How can alter my correspondent banking processes to reduce Financial Crime Risk? • Do all processes require four-eye checks?	• End to end processes to support the customer lifecycle
Organisation & Governance	• How to best organise the business and ensure timely escalation of issues?	• Business, Operations, Technology & Compliance team structure and interaction
People	• How do make sure that right person is assigned to the right job? How do you ensure that resources have knowledge of regulations?	• Role definitions and trainings
Location	• How should I organise my functions (e.g. locally, regionally)?	• Location of teams
Technology	• Can my systems support all regulatory requirements?	• End to end systems which support the customer lifecycle

Key aspects of financial crime operating model

The current financial crime operating model requires a blend of effective governance, specialised skillsets and automated systems capable of handling large volumes of data

Managing internal risk

- Escalation of FCC or AML risks to leadership, AML risk heat maps, regulatory issues, audit and risk assessment outcomes, client / product risk vs business strategy issues



Managing regulatory risk

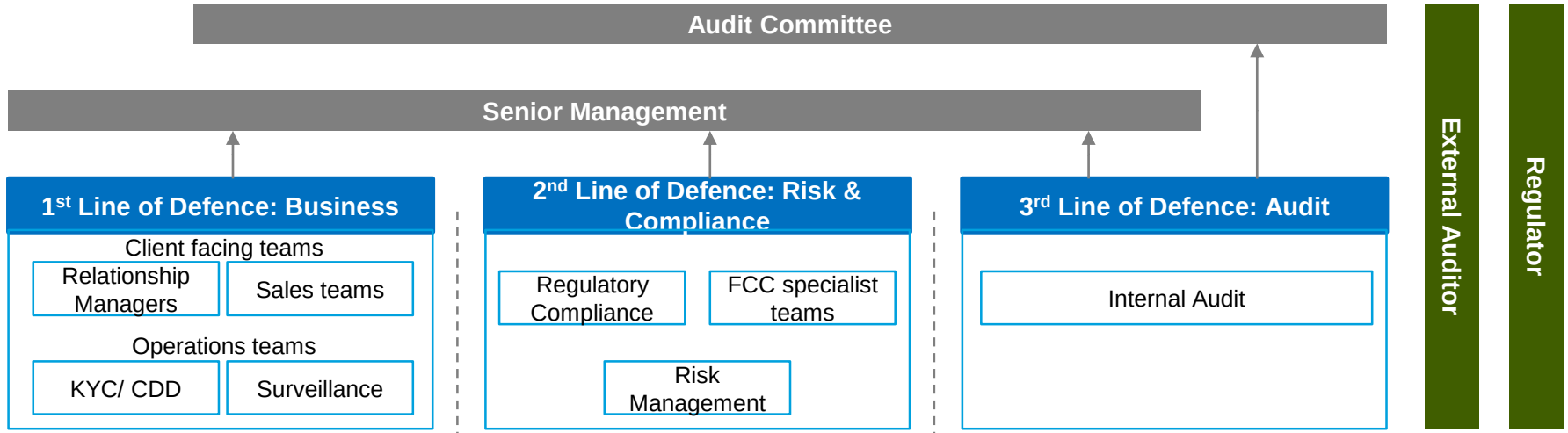
- FCC obligations to have a sound compliance framework
- Responsive to regulatory changes and effective self assessment to remediate or prevent breaches

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Three lines of defence

Three lines of defence must work effectively. The first line needs to be aligned with the risk appetite of the financial institution and second line assurance needs to be enhanced to enable early risk detection ability



- 1st Line of Defence includes the risk owners/ managers who are involved in day to day risk management
- Front line staff are the persons who know most about the customers and their typical pattern of transactions. They are in the best position to identify unusual activities
- The front line staff are supported by the operations teams who perform four eye check on the front line activities (e.g. CDD documentation)

- Designated team independent of the client relationship. Report directly into the senior leadership – arguably limited independence
- Responsible for developing risk management framework and overseeing and challenging current risk management processes
- ***Beefing up and sharpening second line assurance is extremely critical for an FI to be more agile in addressing and closing gaps. FIs do not have the luxury to wait for the internal audit / 3rd line of defense findings***

- 3rd Line of Defence includes risk assurance. This team has greater independence as it reports into Audit Committee as well
- This team performs testing through internal and external auditors and review and refine necessary thresholds based on findings
- Provide an independent perspective and challenge the process

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Compliance risk assessment and risk mitigation (1 of 2)

Risk assessment approach

Assess Across all Entities → Regulatory/Policy Gaps and Process Enhancement Opportunities

Control Effectiveness

- Mapping client's internal policies to regulatory requirements to assess regulatory gaps. For example mapping MAS 626 in Singapore (Prevention of Money Laundering And Countering The Financing of Terrorism – Banks) to the Bank's policies.
- Example areas include: Governance and Oversight, KYC, CDD, ECDD and PEP, Ongoing Monitoring, Reporting & Escalation etc.

+

Inherent Risk

- Information is gathered from each Banking line level to give an overall picture of the enterprise's risk profile across areas such as:
  - Customer demographics;
  - Product offering; and
  - Transactions geography
- Based on the responses gathered, a risk score is given and risk weightages are applied to the risk categories.

=

Residual Risk

- Residual risk is determined by balancing the inherent risk with the overall control effectiveness of the risk management activities and controls.
- The residual risk rating is used to assess whether the risks within the Bank are being adequately managed.

Risk assessment outputs (approach)

Focus Area	Control Effectiveness
AML Governance & Oversight	Satisfactory
KYC and CDD	Deficient
On-going Monitoring	Satisfactory
Name and Sanctions Screening	Deficient
Suspicious Transactions	Satisfactory
Record Keeping	Strong
Staff Training	Satisfactory
Wire Transfer	Needs improvement
Data Protection Exception	Needs Improvement
Overall AML Controls	Satisfactory

	Inherent Risk Area	Inherent AML Risk
1	Customers	High
2	Geographies	Medium
3	Products	High
4	Services	High
5	Transactions	Low
6	Channels	Medium
Overall AML Risk		**High**

Inherent AML Risk	High
AML Controls	Satisfactory
Residual AML Risk	High

Compliance risk assessment and risk mitigation (2 of 2)

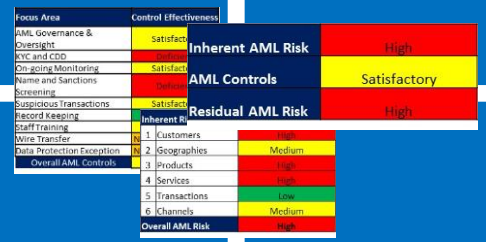
The risk assessment should be used to understand where the source of inherent risk and strategically adjust any levers to better manage the risk associated with clients, geography, products etc.

- Review the sources of inherent risk by reviewing the outputs of the risk assessment
- Review the control gaps and understand how the gaps impact the risks – Inherent and residual

Understand the source of risk and control gaps

Business consensus

- Present the findings to the business stakeholders in visual format so that they understand the processes and controls that they need to address. Obtain buy in from stakeholders



Update Policies & Procedures

- Update policies and procedures to reflect the risk mitigating actions
- Ensure that all impacted parties are aware of the changes in policies and procedures

Adjust Levers and mitigate risks

- strategically adjust any levers to better manage the risk associated with clients, geography, products etc.
- Present the findings to the stakeholders

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Transaction monitoring issues and challenges

1 Internal Controls of Financial Institutions

Inadequate policies and procedures

- Banks generally tackle risks using existing AML compliance policies/ procedures - typically the policies do not explicitly define how the transaction monitoring process should be managed
- Some banks do not clearly define the scope of transaction monitoring

Disorganised documentation

- Banks generally have a central repository to place all related documentation related to a CDD file/alert
- Due to the voluminous amount of documents required to complete due diligence and dispense alerts, as well as amendments to some of the required documents, sifting through documentation to conduct a second-level review is time consuming

Lack of information sharing

- It is necessary to weigh the customer profile against the products traded. However, due to segregation of duties between RM, KYC and transaction clearing teams, open communication and information sharing does not always occur effectively.
- There is lack of sophistication with only basic excel or cognos based reports shared

Inadequate training

- The front line do not have a clear understanding of the risks associated with transaction monitoring alerts hence they do not tend to prioritise the closure
- The operations team reviewing alerts end up sending alerts where they have any confusion rather then performing additional investigation this increasing the workload for business

Staffing shortage

- Many global Financial Institutions are struggling with the large number of alerts being generated from poorly tuned or neglected rules/scenarios whilst not making use of alert tagging, alert rollup or case management capabilities their incumbent transaction monitoring solution
- As all the alerts have to be manually reviewed and closed, workload required has resulted in backlogs

2 Macroeconomics Factors

Cross border privacy restrictions

- Ability to obtain further information on the customer's customer even in cases of suspicious activity may be a challenge due to privacy issues or reluctance of the correspondent to divulge full KYC information available to them.

Lack of transactional data or standardisation

- Payment information does not mandate the input of a comprehensive set of information on the underlying customer (e.g. name, address, registration number, nature of business, etc.).
- Where information is recorded, it is often not standardised (e.g. variations in the same customer name, address, etc.), making data crunching of such information challenging
- The costs involved in setting up such infrastructures is concerning to banks

Transaction monitoring leading practices & considerations

The key industry leading practices have been summarised as follows. In addition, key considerations while managing transaction monitoring system and process have been outlined as well.

Applying the 'right' triggers *(i.e. reflective of internal tolerances, customers, products, geographies)*

Capturing and anticipating emerging threats and new behaviours

Evaluating the 'right' data *(e.g. KYC data, transactions, government lists, etc.)*

Access to reliable test data that allows for benchmarking

Integrating customer risk ratings

Accounting for interdependencies in monitoring rules

Ongoing ability to tune rules and scenarios

Linking transaction behavior to customer profile information

Adequate resourcing of lines of defense *(i.e. technology and staffing)*

Customer segmentation for alerts triaging

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Trade finance key risks & issues

Trade Finance has become a popular instrument for Money Laundering as:

- The tremendous volume of trade makes it easy to hide individual transactions
- The complexity that is involved in multiple foreign exchange/cross border transactions
- The limited resources available to agencies wanting to detect money laundering

Disjointed Information Loop

Effectiveness of CDD / gate keeping (customer Identification, verification and screening)

Technology & Process architecture for trade surveillance (screening and alerts management)

Trade document reviews, consideration of key risks and screening of key parties to the transaction

Customer Life Cycle

Back Office - Management of key client and transaction risk

Front Office – Management of relationship and transaction needs of client

Risk Assessment, internal audit findings and external audit findings

Controlling Persons / FCC Compliance – policies, procedures, exceptions / escalation of risks and training

Operations – transaction documentation, completion of trade, payment, and settlement

Issues	
	• Lack of clear policy & inconsistent approach to risk assessment with no specific trade finance money laundering risk assessment. • Inability to demonstrate that money laundering risk had been taken into account when processing particular transactions. • Trade processing staff do not make adequate use of CDD information gathered by relationship managers or trade sales teams. • Little or no management information on financial crime risks in the trade finance business. • No escalation of potentially suspicious transactions for further review and more senior level sign-off on the basis of ML concerns. Transactions were usually escalated for sanctions reasons or because the value of the transaction had exceeded a pre-determined threshold. • No specific trade finance financial crime training for relevant staff. • Inadequate systems and controls over dual-use goods

Red flags

5 broad categories that should be considered together

1

Customer Red Flags
Engaging in transactions which deviates from regular business strategy or transactions which lack business sense
e.g. Steel company that starts to deal in sugar and paper products frequently

2

Document Red Flags
Encompass abnormality in documentations commonly required in trade finance such as Letter of Credit and Bill of Lading. Incomplete or dubious documents may warrant increased scrutiny and due diligence effort
e.g. Shipment locations of the goods inconsistent with LC; actual shipment occur in high risk country such as Iran

3

Transaction Red Flags
Specific transaction terms and structure which are incoherent with industrial norms and potentially do not make economic sense, such as request to include clauses which seek to benefit buyer/seller
e.g. Complex transaction structure across numerous intermediaries without supporting reasons

4

Payment Red Flags
Terms of payment which appear to be highly unusual or complex and may involve specific clauses to obscure the true identify of the ultimate beneficiary
e.g. Request to pay third party in cash and payment in tax-haven or high banking secrecy jurisdiction such as BVI

5

Shipment Red Flags
Concern about the nature and characteristics of the actual goods to be shipped/received, particularly if shipping method does not make economic sense or highly unlikely due to the weight/quantity/value of the goods
e.g. Using forty-foot container to transport small amount of low-value goods

Changing landscape of trade finance

Regulatory demand for compliance places pressure on business processes. This is particularly difficult in trade finance, due to the need to comply with various regulations imposed by different jurisdictions. The Know Your Customer (KYC) process and regulation to enforce embargoes continue to place a heavy load on trade bankers

- Until fairly recently, compliance in trade finance was limited to the examination of documents
- The traditional view was that the main risk within trade finance is one of fraud

- Now, in addition to document review there is extensive screening – against multiple lists – of data elements embedded in ancillary documents
- Risks classified into 3 categories – embargoes; TF (including fraud); & sanctions/proliferation financing

Screening types		
Screening hits	**Voyage checks**	**Sensitive countries**
• An automated screening utility against a blacklist database comprising organisations, individuals, goods, vessels and countries compiled by regulatory-competent authorities • Measures the resemblance between blacklisted entries and entry in the system. Everything matched within a similarity threshold flagged as a possible “hit”. The Hit can be related to Sanctions or Terrorist Financing	• These checks are performed to manage financial crime risks using Lloyds Intelligence, carrier’s Website, IMB Check etc... Checks include: – Does the shipment exists? - Fraud & AML Risks/ What is the shipping route? - Sanction Risk – Document required include Transport Documents, e.g. B/L or Airway Bill. – Criteria for voyage check depends on Transaction amount ≥ a threshold and/ or red Flags	• Trade Transaction is only a trigger event. • Relationship Level Management where RM performs the Sanction Exposure Review. • Sanction Exposure Review will be sent to RM or designated party.

To survive in this fragile environment, banks must find a way to assemble the various pieces of the jigsaw by making use of streamlined, harmonised processes and smarter application of technology; for example by screening all fields in a SWIFT MT700/760 series message at various stages in the life of an LC and international guarantee, as well as vetting all incoming or outgoing payments for sanctions purposes.

Changing landscape of trade finance

Key issues and key risks

Banks' compliance capabilities and TOM - Trade documents – 100% review, screening, skills and expertise	Robustness of KYC, documents review, red flags embedded in monitoring system and stand alone targeted training
Sanctions linkages – sanctioned country, sanctioned person, sanctioned items / business?	Circumvention techniques assessed
Screening of all parties to a transaction and screening at key stages of transaction	Obtaining payment / transaction information of ultimate purchaser of goods
Trade transactions alerts Monitoring – reporting or stopping a transaction	Red flag – eg : Dual used goods or high risk goods, unusually complex structuring , payment to / from third parties
IMB & Lloyds checks - shipping container numbers are validated	Capabilities of assessing the price? Global customs database? TTU?

Skills of staff, extent of document and underlying transaction review, hits investigated prior to transaction, maintaining a database of prices of similar goods for reference; screening for agents, insurance companies, shippers, freight forwarders, delivery agents, inspection agents, signatories, and parties mentioned in certificates of origin where this information is available, as well as the main counterparties to a transaction

Agenda

1	Key recent regulatory developments
2	Complexities in FCC TOM
3	Three lines of defence
4	Effectively using risk assessments
5	Transaction Monitoring issues and solutions
6	Trade based money laundering
7	Correspondent banking

Industry trends

The future of correspondent banking

Increasing regulatory supervision

Regulators and supranational AML supervisory bodies are recognising the growing threat posed by lax AML controls, and have in recent years issued more prescriptive guidelines for financial institutions/money service bureaus to tackle correspondent banking risks. E.g.:

- MAS Guidance on AML/CFT in Trade Finance and Correspondent Banking (2015) (http://www.mas.gov.sg/News-and-Publications/Monographs-and-Information-Papers/2015/Guidance-on-AMLCFT-Controls-in-Trade-Finance-and-Correspondent-Banking.aspx)
- Wolfsberg AML Principles for Correspondent Banking (2014) (http://www.wolfsberg-principles.com/pdf/standards/Wolfsberg-Correspondent-Banking-Principles-2014.pdf)

De-risking is on the rise

As regulatory scrutiny increases, de-risking is on the rise as banks off-board smaller correspondent bank clients that pose more risk vs. potential returns. This has resulted in a number of socio-economic issues, such as:

- An increase in systemic risk of the banking industry as a whole, as money launderers turn to underground banking systems
- Persons in less developed/developing countries become increasingly segregated from formal banking channels, also driving up compliance costs in such jurisdictions

Third party involvement in addressing regulatory concerns

Third party payment systems are also increasingly involved in addressing of regulatory concerns. SWIFT, the wire payment system used by a majority of banks, is introducing the SWIFT Traffic Profile initiative, which addresses the Know Your Customer's Customer challenge by providing transparency on client's activity over the SWIFT network in high-risk/sanctioned jurisdictions

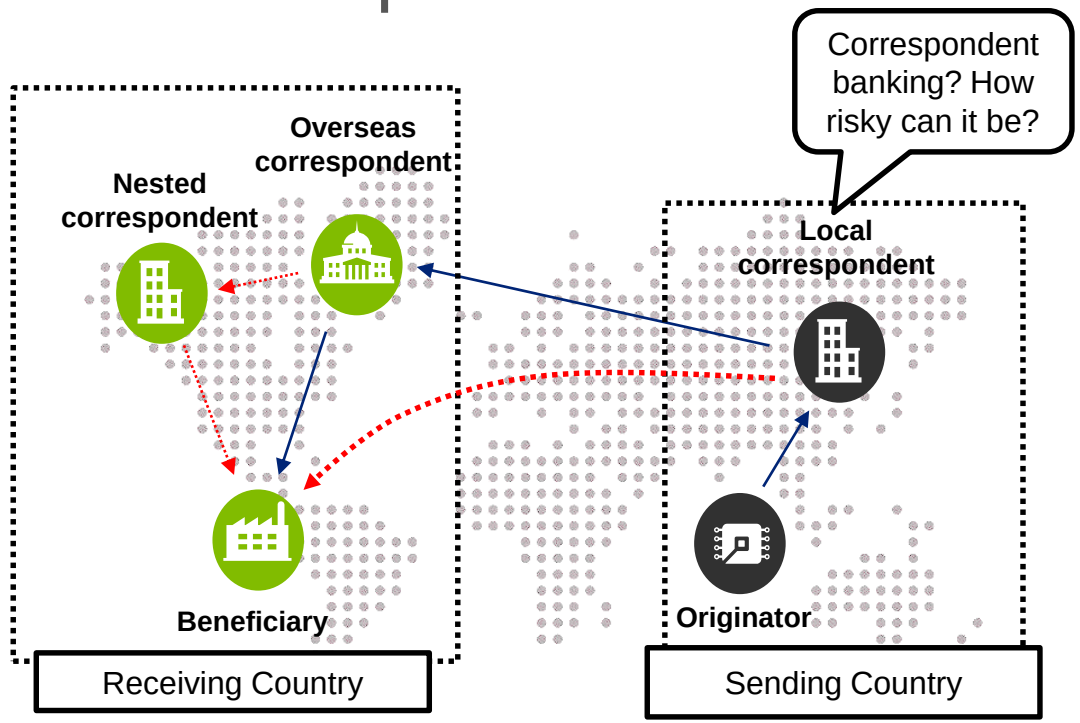
- The system uses customer data provided to uncover flows in where the bank may not be directly involved and those that carry potential downstream correspondent exposure to AML risk.

Correspondent banking AML risks

What risks are our clients exposed to?

Often, our client has no direct relationship with the underlying parties to a transaction and is therefore not in a position to verify their identities – knowledge of the underlying is limited to the extensiveness of the respondent's CDD/KYC controls

Correspondent banks may have a downstream correspondent bank of its own, i.e. this further segregates the correspondent from the underlying parties. Such relationships are known as nested correspondent banking relationships



If due diligence is not conducted extensively, it may not be evident to the client that the correspondents/respondents in the receiving country may have characteristics known to be used by launderers, i.e. the respondent bank:

- is a shell bank
- is an offshore bank
- Is unregulated
- provides payable-through services

Correspondents/ Respondent/ Beneficiary in the receiving country may display other high risk parameters, e.g.:

- located in a high risk/non-FAFT cooperative jurisdiction
- Controlling directors/ shareholders of the bank are PEPs, which have been subject to regulatory enquiry for financial crimes
- etc.

Correspondents often have limited information regarding the nature or purpose of the underlying transactions, particularly when processing electronic payments or clearing cheques.

Evaluating correspondent banking relationship

What are the key CBDD considerations that must be evaluated

Key risk attribute	*Examples (non-exhaustive)*
Geography	• Transactions involving one or more High Risk jurisdictions including US Sanctioned countries • Transactions related to high risk corridors (e.g. transactions from a country known for corruption and high taxes to a low tax country) • FI incorporation and / or operations in high risk jurisdictions with immature AML regulatory regime(s)
Transactional patterns	• Transactions involving four or more jurisdictions without clear rationale • Transactions originating and terminating in the same country after passing through multiple jurisdictions • Transactions where the originator name and beneficiary name are the same but with different addresses • Transactions to jurisdictions where the foreign financial institution has no known business activities or interests • Customer of the correspondent bank has an unusually large number of transactions sometimes with further information in the instructions identifying the nested customers
Management / Control & FI's AML/CFT Standards	• History of AML related regulatory penalties for either witting or unwitting correspondent banking lapses • Adverse media pertaining to financial crime allegations / convictions of the Bank's management and / or compliance personnel • Lack of transparency in location of owners and / or their corporate legal structures • Lack of evidence that the FI is listed on a reputable exchange or governed by a satisfactory regulatory authority • High degree of control / involvement by Politically Exposed Persons in management of the FI • Downstream FIs' incorporation and regulation status cannot be confirmed (i.e. high risk for shell banks)
Products / Services	• Complex Trade Finance instruments involving higher risk jurisdictions and / or industries • Downstream access by Money Services Businesses • Transactions involving known high risk goods (e.g. chemicals) and / or vague descriptions of goods (e.g. scrap) • Gaps in understanding of ultimate downstream users of the product / services for higher risk FIs • Downstream FI allowance for payable-through-accounts • Pouch activities reflective of sequentially numbered transactions, amounts under 3,000 or 10,000, little or no purchaser information, repetitive beneficiaries or originators or both, round even dollars
Transactional processing	• FI exceeds the expected value / volume stated in its client profile for funds transfers • Attempts to re-process previously declined transaction for the same amount but with different counterparties recorded in the transactional details
High risk terms	• References to "charity" "charitable" "foundation" in transactional instructions (e.g. MT202s)

Correspondent banking: Risks typologies

	Examples of red flags/risk typologies:
KYC/ CDD	• Does not recognise correspondent banking relationships, though it clearly provides services that require a respondent bank overseas (e.g. trade finance, clearing and liquidity services) • Policies/procedures for CDD/KYC of correspondent/respondent banks does not meet minimum regulatory standards, and/or does not require heightened due diligence on correspondent/respondent banking relationships • Has been the subject of regulatory scrutiny for lapses in AML controls, particularly with regard to transactions or CDD/KYC shortfalls with other financial institutions • Does not have policies and procedures to mitigate the risks posed by downstream correspondent banking • Procedures do not mandate the screening or identification of the underlying parties in the electronic payments/transfers (e.g. SWIFT) • Is located in a non-FATF compliant jurisdiction, or a jurisdiction known to have heightened ML/TF risks • Is not regulated by a supervisory authority in a FATF-compliant jurisdiction • Does not have a physical presence, or provides services to shell banks • Is located outside the country where the correspondent bank account is set up, and domiciled in a well known tax haven, or provides services to offshore banks • Management or controlling shareholders of the bank are PEPs, in particular those with previous records of financial crime allegations • Lack of transparency over identity of management/controlling shareholders • Provides correspondent banking services but does not adequately share information on their clients • Provides services that require an overseas correspondent bank (e.g. trade finance, forex clearing and liquidity services), but claims it does not provide correspondent banking relationships. • Has been the subject of regulatory scrutiny for lapses in AML controls, particularly with regard to transactional or CDD/KYC shortfalls pertaining to other financial institutions • Potential lapses in CDD/KYC and transaction monitoring policies and procedures, including: – No requirement to conduct heightened due diligence on correspondent banking relationships, and subject such accounts to more frequent monitoring – Operating instructions do not mandate the screening or identification of the underlying parties in the electronic payments/transfers (e.g. SWIFT payments, Fedwire)
Alerts	• Purpose of transaction (or other transactional details) does not commensurate with expected account behaviour and/or the nature of business of the underlying clients • Information in the transactional details appear to be missing or removed (stripping) • Transactions pass through multiple jurisdictions without a legitimate purpose • Structured transactions: Transactions that are structured to multiple payments to avoid triggering the stipulated threshold

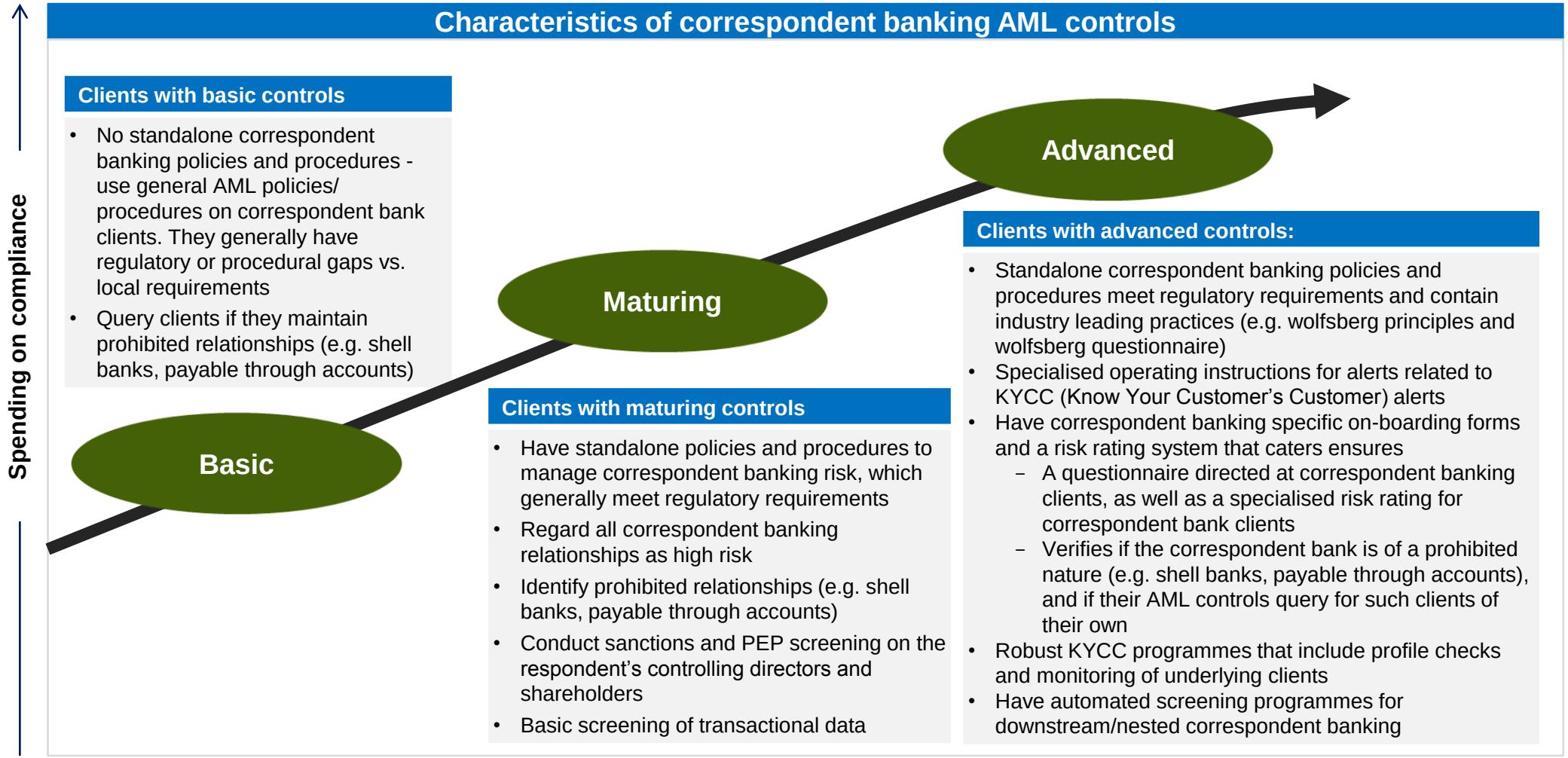
Managing correspondent banking relationships

The following are measures FIs have to implement to mitigate CB risk, according to recent directives by MAS and Wolfsberg

Area of risk	Directive provided
Geographic risk	Review pronouncements from regulatory agencies and international bodies to evaluate the geographic risk presented by the jurisdiction where the client is based or headquartered Enhanced CDD should be performed on clients based in strategic AML/CFT deficiencies
Branches, Subsidiaries and Affiliates (of clients)	For group relationships, due diligence should extend to branches and subsidiaries within the group. Where the relationship is solely with an affiliate of the group, due diligence should extend to the parent entity.
Ownership and Management Structures	Ownership and management structure of the Correspondent Banking Client may present increased risks, and should be examined in detail
PEP Involvement	If a PEP appears to have involvement in the Correspondent Banking Client, then the institution shall ensure it has an understanding of the risk they may present to the relationship
Regulatory Status and History	The client's regulated status should be determined Independent sources should be referred to in verifying if the client has been the subject of any relevant, material regulatory action
Nested/ Downstream Correspondents	Banks should put in place a process to identify and assess risks posed by nested/downstream relationships, including: – Obtaining a list of downstream clearers – Assessment of controls of AML/CFT controls of downstream correspondent clearers

Maturity of correspondent banking controls

The key characteristics by maturity for Financial Institutions providing correspondent banking services have been summarised as follows:



Conclusion

Risk based approach?
Key considerations …

From an AML/CFT perspective, a risk based assessment involves identifying key indicators where the FI needs to perform a deep dive analysis to address any potential risks the organisation can be exposed to and the sufficiency of controls in place to manage such risk.

The regulatory bar on FIs particularly in the more mature and developed markets has risen so much today that “risk based approach” translates to “heightened risk based approach” when designing AML / CFT frameworks and assessing associated risks and controls.

Compliance frameworks need simply to be prudent and defensible in today’s regulatory environment.

FIs need robust regimes to not only identify risks at the point of onboarding but monitor such risks throughout the lifecycle of the customer with the FI.

The outcome of the risk assessment must, and it is critical that it does, inform the overall framework, policies, procedures, process architecture, people, technology, customer risk profiling, monitoring and assurance exercise as well as help design the MLRO’s dashboard to his management.

Compliance programmes and frameworks that are well defined must continually challenged and modernised / enhanced, new threats and emerging typologies and associated red flags duly embedded in the framework

Take a strategic view of the outcome of the risk assessment as well as the underlying information and trends seen from it – don not just focus the inherent and residual risk.

Sharpen second line of defence assurance programme for early detection and timely resolution of issues

To further manage risk, monitoring of customer behaviour taken into account to reassess risk profiling / rating, robust decision making on and de-risking of 'risky customers' whose risk is difficult to manage for the FI and maintenance of a register for refusal of onboarding and exit of business relationships due to AML / CFT risks.

Speaker profile

Radish Singh
SEA Anti-Money Laundering & Sanctions Leader
radishsingh@deloitte.com

Radish leads the Regulatory Advisory – Financial Crime, Anti-Money Laundering (AML), Sanctions and Know-Your-Customer (KYC) – practice within Deloitte Forensic in Singapore and Southeast Asia. With over 17 years of experience, Radish is a subject matter expert on advising financial institutions on financial crime. She has been actively presenting on global regulatory reform to major banks and institutions in Singapore as well as in various public forums. Her clientele currently incudes major global and local banks in Singapore. She has also previously led an engagement with the Association of Banks in Singapore to revise and modernise their AML guidelines for the banking industry in Singapore. She has also advised the Institute of Banking and Finance Singapore on revising their compliance and AML industry standards modules.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 150 countries, Deloitte brings world-class capabilities and highquality service to clients, delivering the insights they need to address their most complex business challenges. Deloitte's more than 225,000 professionals are committed to making an impact that matters. Deloitte serves 4 out of 5 Fortune Global 500® companies.

About Deloitte Southeast Asia
Deloitte Southeast Asia Ltd – a member firm of Deloitte Touche Tohmatsu Limited comprising Deloitte practices operating in Brunei, Cambodia, Guam, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Singapore, Thailand and Vietnam – was established to deliver measurable value to the particular demands of increasingly intra-regional and fast growing companies and enterprises.

Comprising 270 partners and over 7,300 professionals in 25 office locations, the subsidiaries and affiliates of Deloitte Southeast Asia Ltd combine their technical expertise and deep industry knowledge to deliver consistent high quality services to companies in the region.

All services are provided through the individual country practices, their subsidiaries and affiliates which are separate and independent legal entities.

About Deloitte Singapore
In Singapore, services are provided by Deloitte & Touche LLP and its subsidiaries and affiliates.