Singapore's Money Laundering National Risk Assessment (ML NRA)

Key Highlights for Financial Institutions
July 2024



Introduction to ML NRA

- **Developed as part of Singapore's continuing efforts to maintain effectiveness of our anti-money laundering (AML) regime, amidst changes in risk landscape andin line with FATF best practices.**
- **Complements tools in place to support authorities and industry in taking risk-focused and proportionate measures to prevent illicit actors from abusing our system.**
- **Synthesises and updates Singapore's understanding of key ML threats and risks, and include:**
  - Observations and risk assessments by agencies across the Government
  - Feedback from private sector entities and foreign authorities
- Conducted under auspices of AML/CFT Steering Committee (comprising Permanent Secretary of Ministry of Home Affairs, Permanent Secretary of Ministry of Finance and Managing Director of the Monetary Authority of Singapore), which leads Singapore's overall efforts in anti-money laundering, countering of financing of terrorism and countering proliferation of financing (AML/CFT/CPF).
- Driven by the Risks and Typologies Inter-agency Group (RTIG), the working group tasked to monitor and review risks at the whole-of-government level:
  - Includes Singapore's Financial Intelligence Unit (FIU – Suspicious Transaction Reporting Office (STRO)), law enforcement, regulatory, supervisory and policy agencies involved in AML/CFT work in Singapore.
  - RTIG regularly discusses Singapore's key ML threats and risk considerations, including cases, typologies and vulnerabilities, and recommends mitigation steps.

Changes since the last ML NRA

- **Since the last published ML NRA, Singapore has been closely monitoring our ML risks,** including through:
  - **Conducting thematic risk assessments** – such as for the abuse of legal persons, terrorism financing, virtual assets (or digital payment tokens), environmental crime ML
  - **Working with industry** (e.g. through AML/CFT Industry Partnership (ACIP), Association of Banks in Singapore (ABS), Association of Crypto Currency Enterprises and Start-ups Singapore (ACCESS), Remittance Association Singapore (RAS), Singapore Trustees Association (STA) etc.), engagements by agencies, publication of best practices and guidance papers) to raise collective risk awareness.
  - **Risks have become more complex,** due to geo-political climate, macro-economic events, and increased use of sophisticated structures

"New" sectors not covered in previous ML NRA
• Digital Payment Token Services Providers • Precious Stones and Precious Metals dealers

Overview – Structure of ML NRA report

ML NRA contains two key sections:

1 Overall ML Threats assessment

- Contains an overview of key national ML threats
- Includes foreign ML threats and domestic ML threats
- In assessing threat level, takes into account a broad range of quantitative and qualitative indicators, including:
  - cases, prosecutions, convictions, Suspicious Transaction Reports (STRs), international cooperation requests
  - Singapore's inherent exposure based on surveillance, contextual factors, including insights and observations from regional/global typologies and relevant reports.
  - Incorporates feedback from key foreign partners on ML threats

2 Sectoral Risks Assessment

- Covers sectors subject to AML/CFT obligations, both financial and non-financial (or Designated Non-Financial Businesses and Professions).
- Each sector's ML risks take into account:
  i. Exposures to ML threats,
  ii. Vulnerability assessment, and
  iii. Strength of AML/CFT controls
- ***Being assessed as higher risk means a sector faces greater threats or vulnerabilities, but does not necessarily mean it has weak controls***
  - **ML threats** are weighted most heavily, followed by inherent **vulnerabilities**
  - While controls are important, we have weighted them less in assessing sectoral risks – to reflect that strong controls may not fully deter ML activities, given changing typologies and methods. This also ensures sectors remain vigilant.

- **Guides WOG AML efforts towards more risk targeted law enforcement, supervision and outreach**
- **Informs private sector of key risks (which they can take reference from in assessing risks and enhancing controls and risk mitigation)**
- **Over 50 case studies and box stories, to provide a range of practical examples across sectors**

Money Laundering Threats

KEY ML THREATS

Fraud, *particularly cyber- enabled fraud*

- High number of cases from foreign fraud
- *Marked increase in threat from cyber enabled fraud targeting Singapore residents by overseas syndicates*
- *Threat exacerbated by advancements in digitalisation - key crime of concern globally*
- *Key threat highlighted by other jurisdictions through engagements with foreign authorities*
- *E.g. case studies #2, #3, #6, #10, #11*

Organised Crime, especially illegal online gambling associated with foreign organised criminal groups

- *Layering of illicit funds through multiple jurisdictions*
- *Assets seized/prohibited from disposal in recent major ML case are suspected to be proceeds from illegal online gambling*
- *E.g. case studies #4, #20*

Corruption, *originating from abroad*

- *Inherent threat due to Singapore's geographical location*
- *Facilitated through intermediaries such as banks and legal persons*
- *e.g. case studies #14, #25*

Tax Crimes, *originating from abroad*

- *Inherent threat as wealth management hub*
- *Increase in number of incoming foreign requests, related to tax offences*
- *Legal persons/arrangements and complex structures used to hold and move funds and assets*
- *E.g. case studies #1, #8, #24*

Trade-based money laundering

- *Inherent threat as trading and transportation hub*
- *Increase in requests from foreign counterparts*
- *Involve techniques such as over/under invoicing of good, and use of financial and professional intermediaries*
- *E.g. case study #10, Box Story 1*

OTHER NOTABLE ML THREATS

Environmental Crime

Cyber-crime

Drug-related offences

Sectoral risk assessments – Higher ML Risks Sectors

HIGHER ML RISK SECTORS

(Similar to many other international financial centres) Banks pose highest ML risks to Singapore:

- Inherently exposed to key ML threats, given their role in facilitating transactions in the financial system
  - Illicit funds flowing into or through Singapore are most commonly laundered via bank accounts.
  - Transnational crime syndicates exploiting the banking sector as a destination or transit point for the proceeds of crime (e.g. relating to syndicated fraud and scams, corruption etc.).
  - Exploited by criminals through various ways including rapid pass-through transactions. involving cross border fund flows, conduits such as corporate and individual mule accounts, shell companies.
- Larger proportion of higher ML risks customers, including customers from higher risks jurisdictions, high-net-worth individuals, politically-exposed persons
- High volume of transactions and wide networks through which cross-border transactions can be conducted
- Banks are thus expected to maintain robust AML/CFT controls commensurate with risks. In spite of strong controls, ML threats for banks is high and banks are commonly featured in known domestic, regional and international ML typologies.

Sectoral risk assessments – Higher ML Risks Sectors

HIGHER ML RISK SECTORS

Other higher ML risks sectors are susceptible, in spite of controls in place, due to (i) abuse by virtue of their roles as professional / financial intermediaries, (ii) exposure to cross-border transactions, and/or (iii) placement in high value assets

Corporate Services Providers

- Role in providing upstream services such as incorporation of companies
- Linked to misuse of legal persons in some instances - legal persons are featured in ML cases, including fraud, corruption/tax ,TBML

Digital Services Token Services Providers

- Increased in reported cases related to Digital Payment Tokens (DPTs)
- Relatively nascent sector
- International typologies noted ways in which DPTs can be exploited for cross border transactions

Real Estate

- High value, good store of value and provides opportunity to launder funds
- Typologies related to fraud, corruption/tax ML risks

Casinos

- Cash intensive, exposure to foreign customers, source of wealth or funds from overseas
- Typologies indicate inherent ML threats

Precious Stones and Precious Metal Dealers

- Good store of value, cash focused
- Typologies indicate inherent threats

Payment Institutions Offering Cross Border Money Transfers

- Cross-border activities; exposure to higher risks customers
- Typologies indicate misuse, including by shell companies, for movement of funds across borders

Licensed Trust Companies

- Exposed to higher risks customers, including those with corruption/tax evasion ML risks
- Deal with complex structures (featuring legal arrangements), high value, and cross-border transactions

External Asset Managers (EAM)

- Exposed to higher risks customers including those with corruption/tax evasion ML risks
- Deal with complex structures, high value, and cross-border transactions

What the ML NRA means for FIs?

Financial Institutions (FIs) are required to identify and assess ML/TF risks on an enterprise-wide level, which should incorporate the findings of Singapore's ML/TF National Risk Assessments

ML NRA

Enterprise-wide level ML risk assessment:

- Includes a consolidated assessment of ML risks that exist across all the FI's business units / activities in or outside of Singapore.
- Forms the basis of FIs' overall risk-based approach and will enable FIs to understand its vulnerabilities to ML risks
- FIs' risk assessments should be duly documented and kept up-to-date

FIs' risk-based approach:

- Comprise adequate policies, procedures and controls to mitigate the ML risks
- Guide the allocation of AML/CFT resources within FIs entities (e.g. pay more attention to areas of higher threats/vulnerabilities)
- Assess effectiveness of risks mitigation procedures and controls on an ongoing basis.

What the ML NRA means for FIs?

When performing the enterprise-wide ML/TF risks assessment, **FIs should take into account findings from the ML NRA, including (i) key ML and notable threats, and (ii) financial or non-financial sector that has been identified as presenting higher ML risks.**

Nature and extent of AML/CFT risk management systems and controls should be commensurate with the ML/TF risks identified via the enterprise-wide ML/TF risk assessment process. In particular, FIs should also:

- Incorporate ML NRA findings on **higher risk sector results** into their customer risk assessment process as well
- Consider findings on **key ML threats, including crime types, typologies highlighted in the ML NRA** when performing on-going monitoring of the conduct of customers' account and scrutiny of customers' transactions
- Strengthen engagement and collaboration with authorities (e.g. through public-private partnerships)
- Develop and deploy use of data analytics and other advanced detection techniques to identify bad actors

END

