This is not an ADB material. The views expressed in this document are the views of the author/s and/or their organizations and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy and/or completeness of the material's contents, and accepts no responsibility for any direct or indirect consequence of their use or reliance, whether wholly or partially. Please feel free to contact the authors directly should you have queries.

# Transaction Monitoring

April 2024

# Administration

- Please mute your microphones when not speaking 🔇
- Have your mobile phone handy
- Use the group chat if you wish to comment or ask questions
- Raise your hand if you have questions, and unmute yourself
- Parking Lot
- Co-creation of Content
- Participate actively
- Have fun
- Participation Certificate

# Have Burning Questions?

https://app.sli.do/event/cUwyq4kBsmG5JqHhxzhWpR

Join at slido.com: #2286357

(live until 11 April 2024)

# Correspondent Banking and the Practical Approach to AML/CFT

Module 1 - Correspondent Banking – An Introduction

Module 2 – Fundamentals of Customer Due Diligence

Module 3 – Sanctions and Terrorist Financing

Module 4 – Enterprise-Wide Risk Assessment

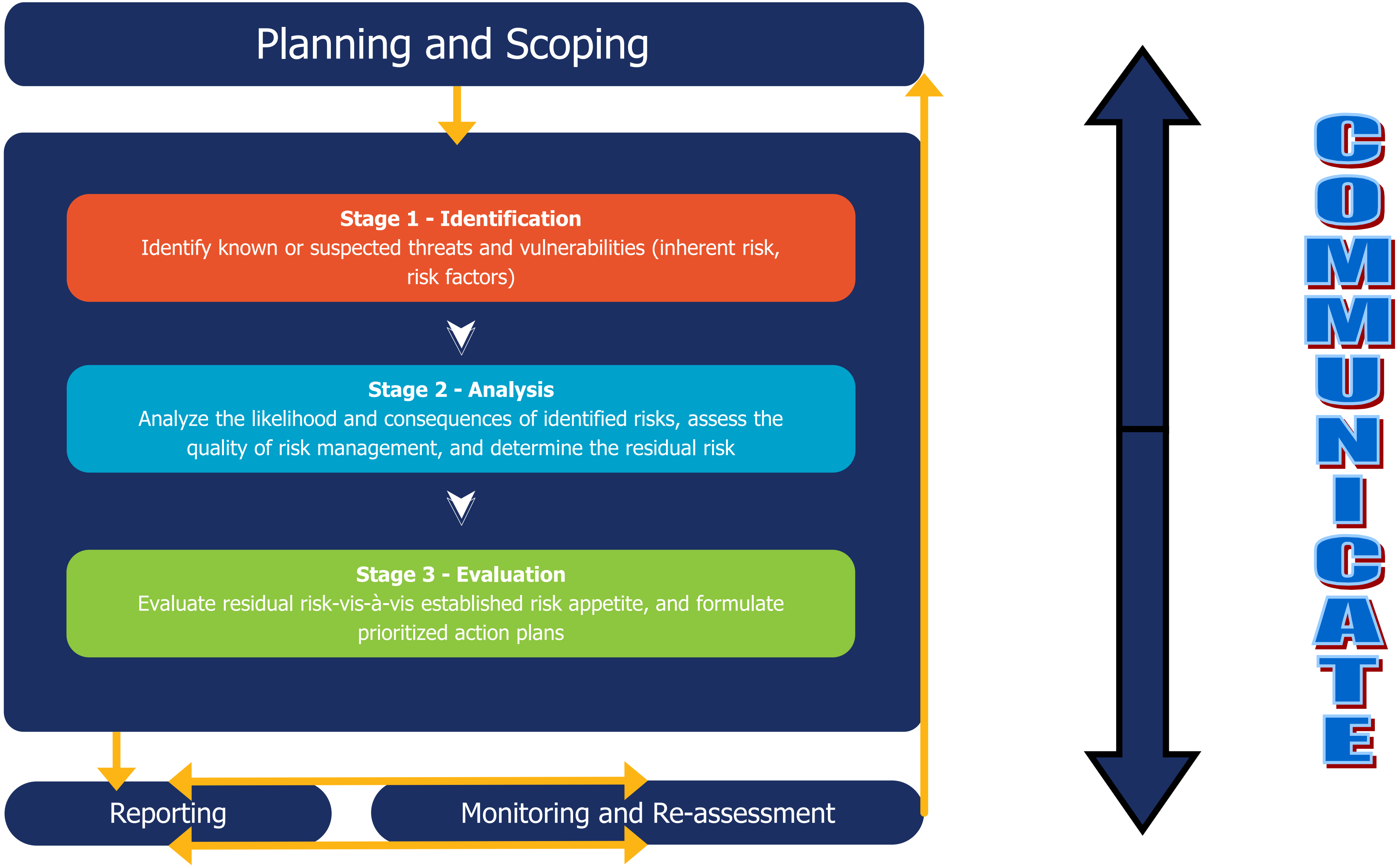
**Module 5 – Transaction Monitoring**

Module 6 – Anti-Bribery and Corruption

Module 7 – Suspicious Transaction Investigation and Reporting

# Recap of Module 4

# The Risk Assessment Process



Planning and Scoping

**Stage 1 - Identification**
Identify known or suspected threats and vulnerabilities (inherent risk, risk factors)

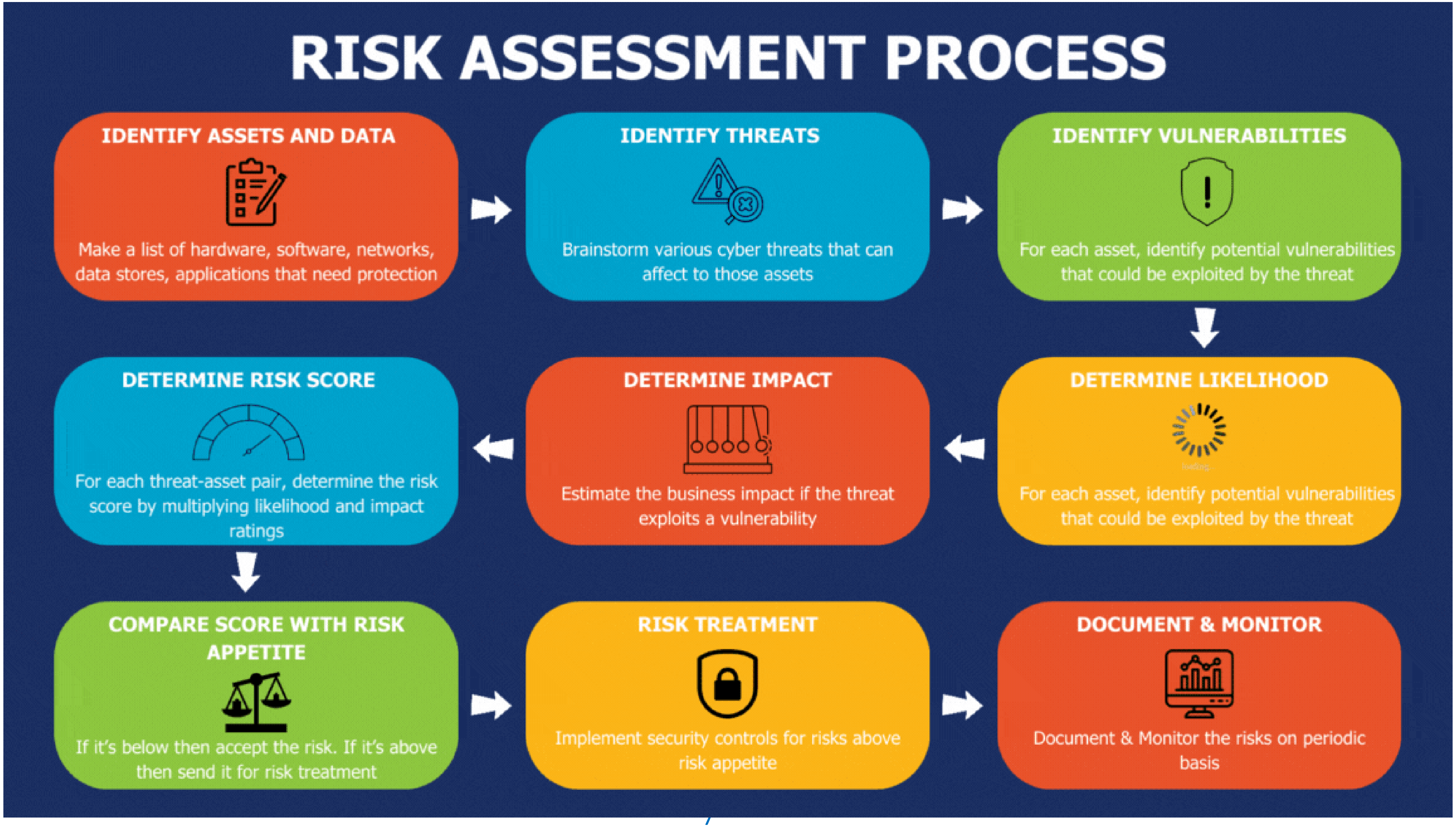
**Stage 2 - Analysis**
Analyze the likelihood and consequences of identified risks, assess the quality of risk management, and determine the residual risk

**Stage 3 - Evaluation**
Evaluate residual risk-vis-à-vis established risk appetite, and formulate prioritized action plans

Reporting

Monitoring and Re-assessment

COMMUNICATE



# RISK ASSESSMENT PROCESS

### IDENTIFY ASSETS AND DATA

Make a list of hardware, software, networks, data stores, applications that need protection

### IDENTIFY THREATS

Brainstorm various cyber threats that can affect to those assets

### IDENTIFY VULNERABILITIES

For each asset, identify potential vulnerabilities that could be exploited by the threat

### DETERMINE LIKELIHOOD

For each asset, identify potential vulnerabilities that could be exploited by the threat

### DETERMINE IMPACT

Estimate the business impact if the threat exploits a vulnerability

### DETERMINE RISK SCORE

For each threat-asset pair, determine the risk score by multiplying likelihood and impact ratings

### COMPARE SCORE WITH RISK APPETITE

If it's below then accept the risk. If it's above then send it for risk treatment

### RISK TREATMENT

Implement security controls for risks above risk appetite

### DOCUMENT & MONITOR

Document & Monitor the risks on periodic basis

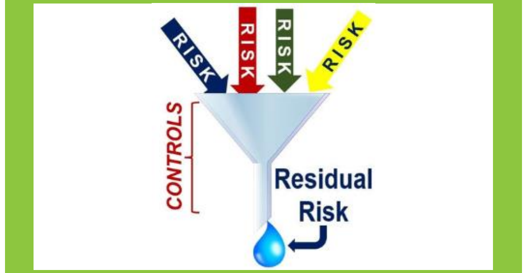
# Phases in Risk Assessment Exercise

Financial crime risk assessment is the first step in managing the risks associated with financial crime. Design of a risk assessment framework will depend on the complexity and structure of an organization, the markets and countries in which it is active as well as its client base.

According to the Wolfsberg Group, a three-phased approach, which it terms as the "conventional/standard methodology," can be adopted in order to undertake a risk assessment.

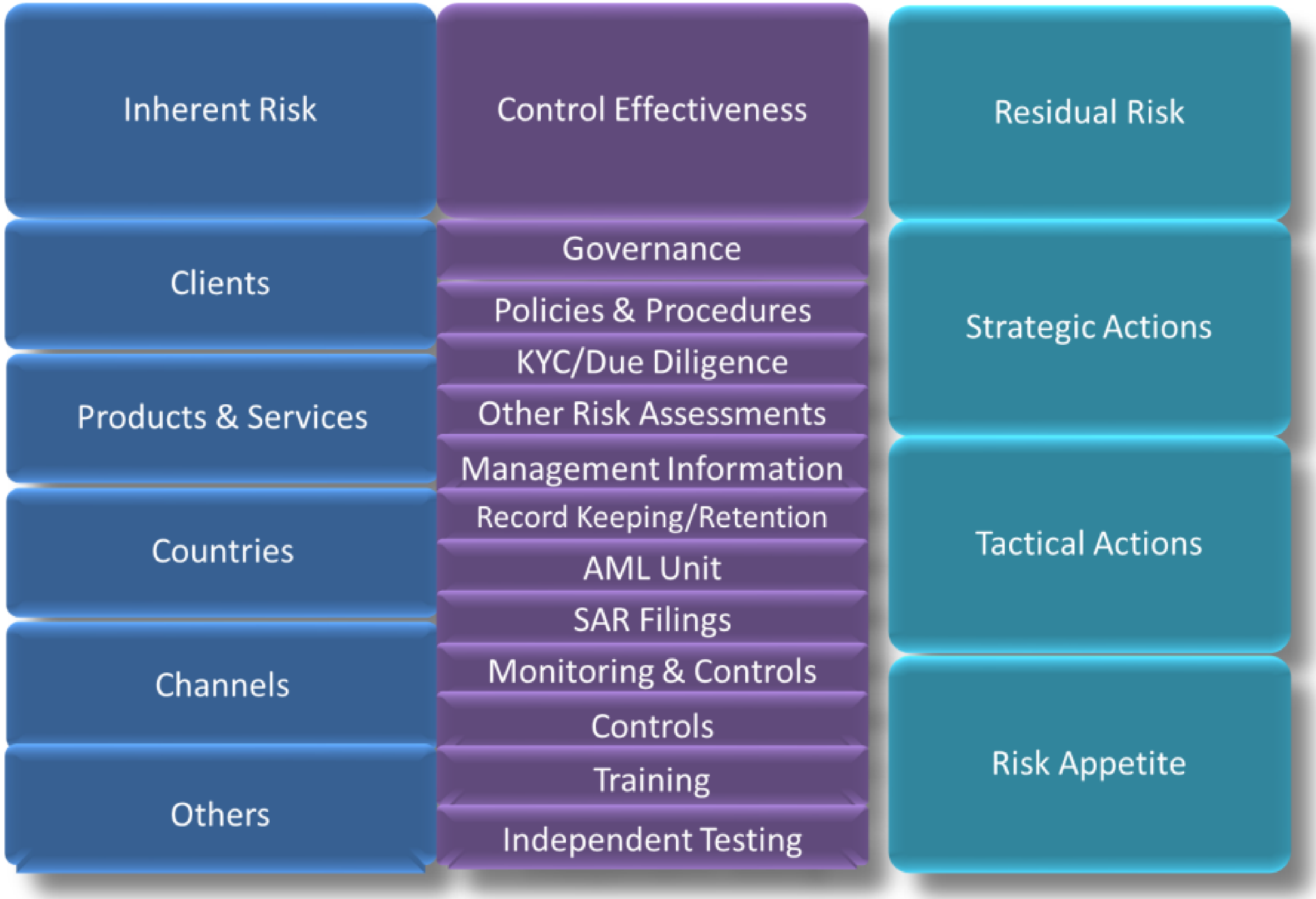
**Phase 1 – Inherent Risk**

**Phase 2 – Internal Control Assessment**



**Phase 3 - Residual Risk Assessment**

# Conventional/Standard ML Risk Assessment Methodology



Inherent Risk

Clients

Products & Services

Countries

Channels

Others

Control Effectiveness

Governance

Policies & Procedures

KYC/Due Diligence

Other Risk Assessments

Management Information

Record Keeping/Retention

AML Unit

SAR Filings

Monitoring & Controls

Controls

Training

Independent Testing

Residual Risk

Strategic Actions

Tactical Actions

Risk Appetite

Source: The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption

# Risk Assessment Matrix

| Inherent Risk<br>Effectiveness Of<br>Control | Low Risk | Medium-Low | Medium | Medium-High | High Risk |
|---|---|---|---|---|---|
| **Low** | Medium-Low | Medium | Medium-High | High | High |
| **Moderate** | Low | Medium-Low | Medium | Medium-High | High |
| **Substantial** | Low | Medium-Low | Medium | Medium-High | Medium-High |
| **High** | Low | Medium-Low | Medium-Low | Medium | Medium-High |
| **Very High** | Low | Low | Medium-Low | Medium | Medium |

ADB

# Practical considerations

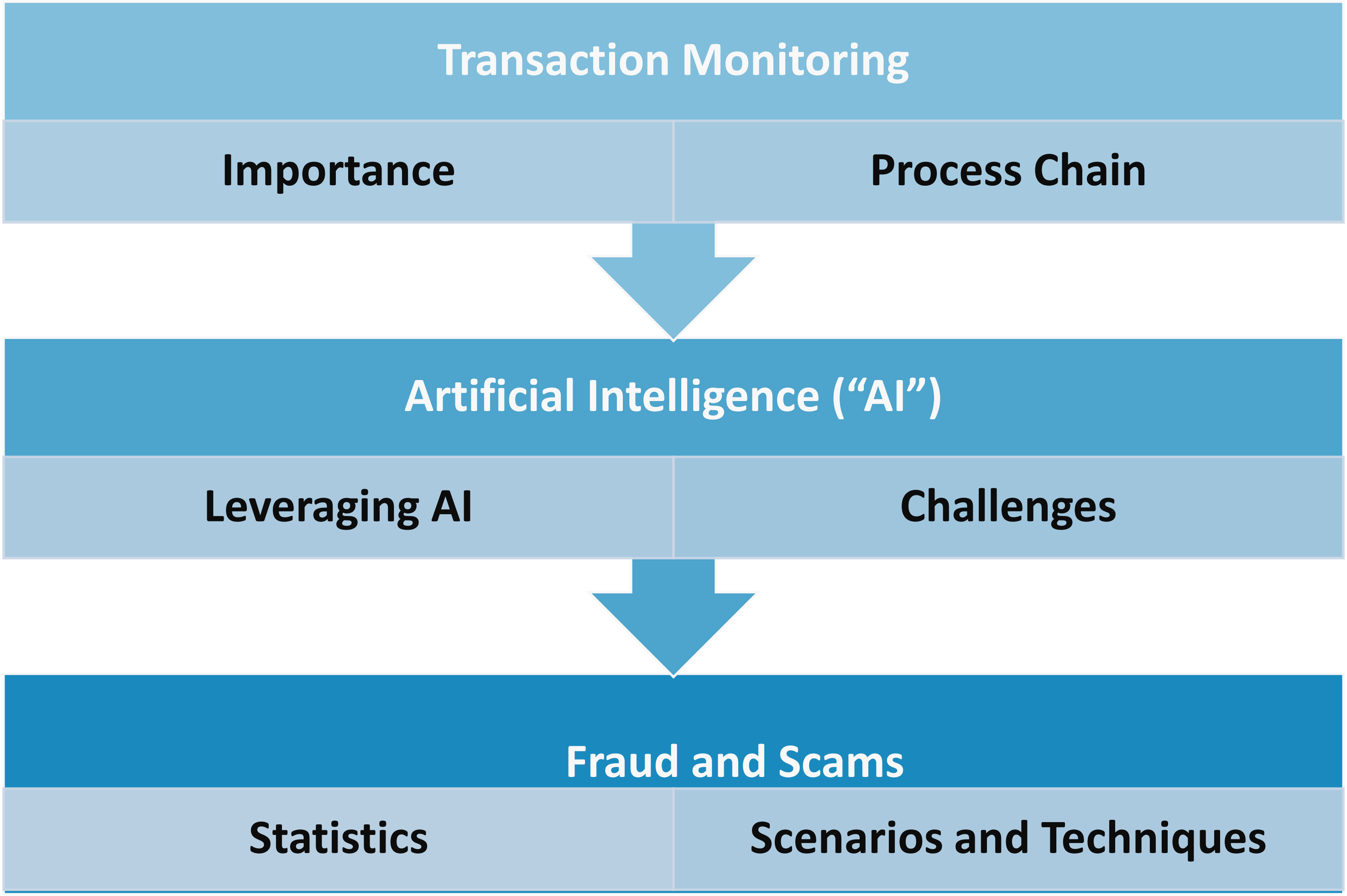
- **Robustness of Methodology** - must address process, scope, roles & responsibilities, record retention, exceptions and approvals, Reporting and review etc.

- **Involvement with Functional Business Areas** - need basic or foundational understanding of the various business and operational areas across the enterprise. It is critical to engage the business units because as the first line of defence these areas have ownership of the risks.

- **Data issues** - . Incorrect or duplicate data can severely impact the risk assessment exercise.

- **Tools** - Customized templates built in standard spreadsheet to sophisticated database systems built in-house or purchased from vendors

# Learning Objectives of this module



Transaction Monitoring

Importance | Process Chain

Artificial Intelligence (“AI”)

Leveraging AI | Challenges

Fraud and Scams

Statistics | Scenarios and Techniques

# Financial Crime Offences

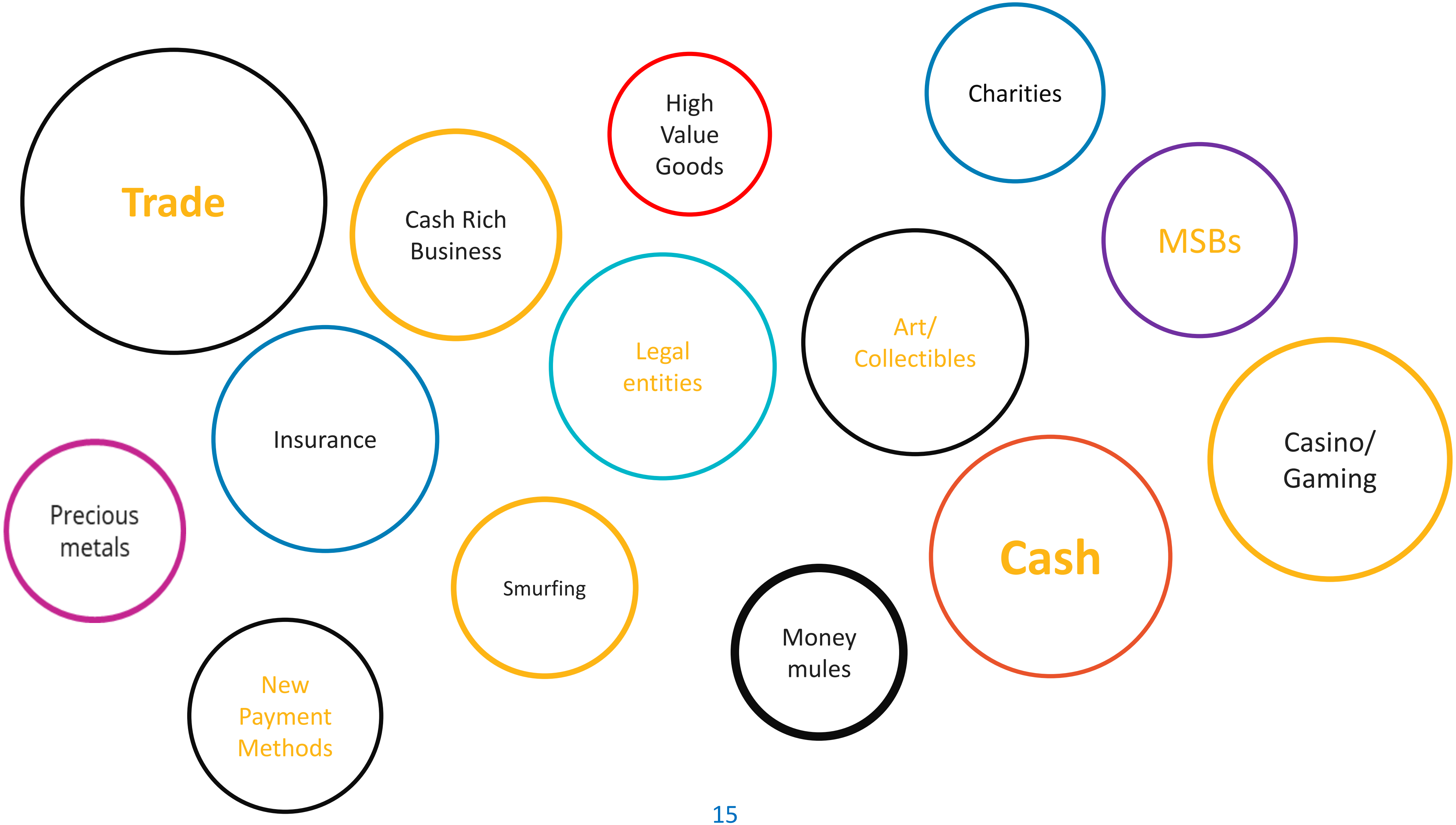
Basic types of conduct at the core of financial crime offences in commerce and industry, trade and profession.

Money laundering is a consequence, not a primary criminal activity

- Crimes committed on the business or persons
- Crimes committed by the business or persons
- Crimes relating to the existence, structure and founding of the business
- Crimes committed using the business as vehicle

Photo illustration

# Common Ways to Launder Money



Trade

Cash Rich Business

High Value Goods

Charities

MSBs

Legal entities

Art/ Collectibles

Insurance

Precious metals

Casino/ Gaming

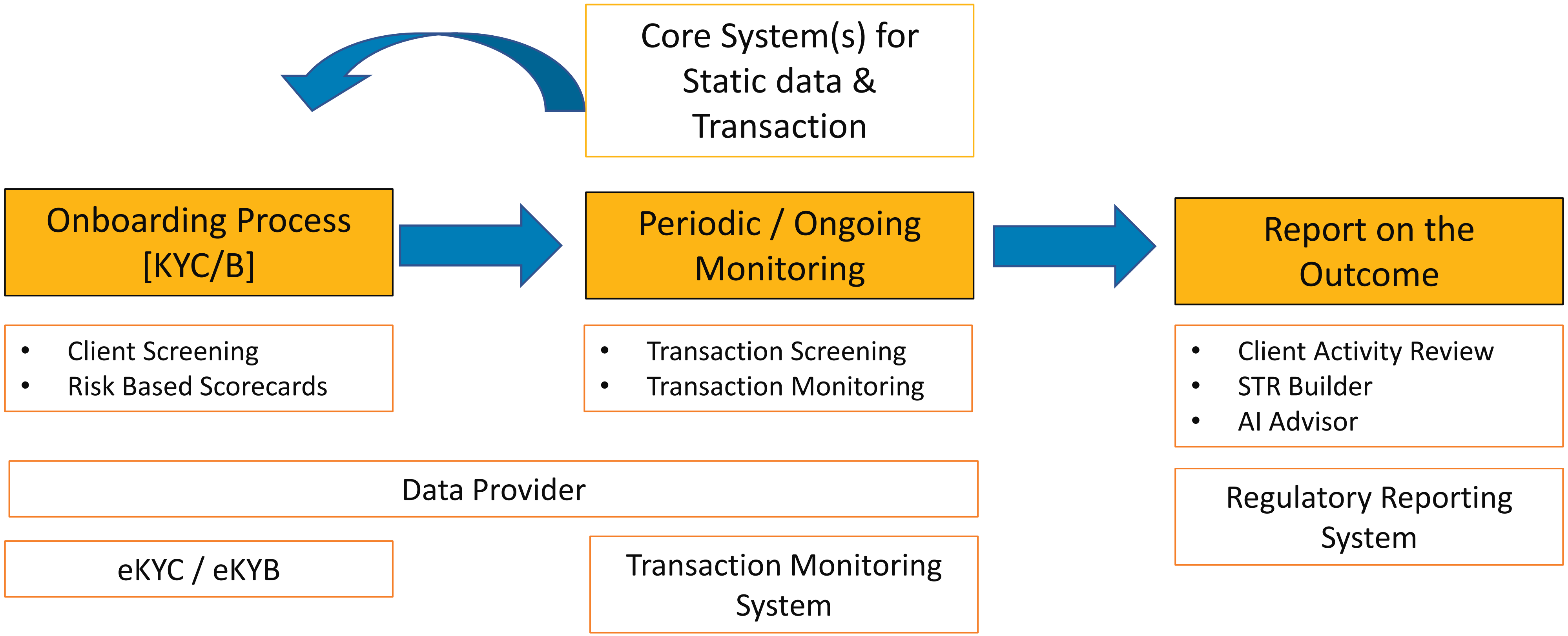
Cash

Smurfing

Money mules

New Payment Methods

# Customer Due Diligence Process



Core System(s) for Static data & Transaction

Onboarding Process [KYC/B]

- Client Screening
- Risk Based Scorecards

Periodic / Ongoing Monitoring

- Transaction Screening
- Transaction Monitoring

Report on the Outcome

- Client Activity Review
- STR Builder
- AI Advisor

Data Provider

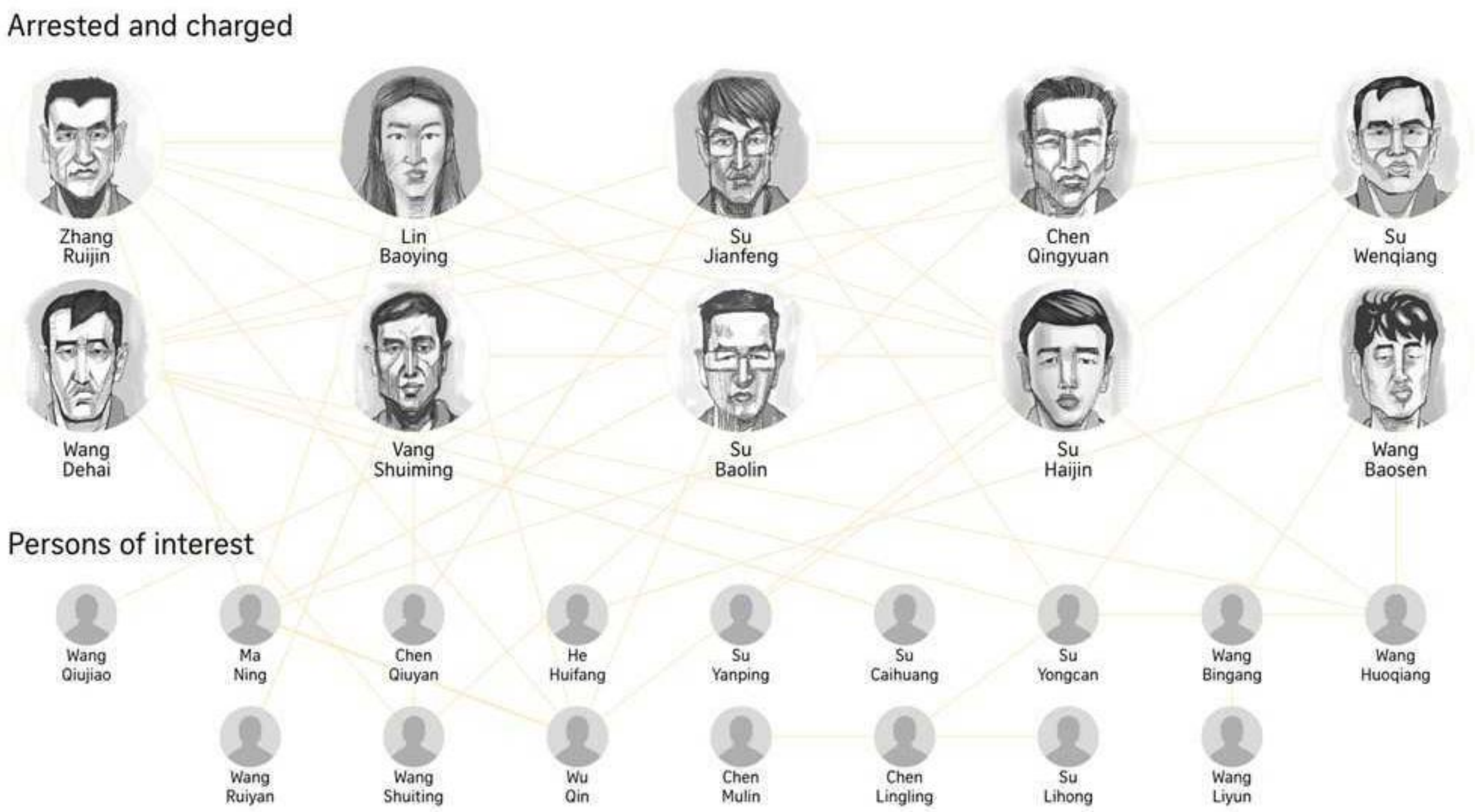
eKYC / eKYB

Transaction Monitoring System

Regulatory Reporting System

# Singapore – August 2023 Headlines

## S$3 Billions worth of assets seized and still counting …



Name: Su Wenqiang

Age: 31

Nationality: Originally from China, holds a Cambodian passport

Charges: 11

Money laundering accused on the run from Chinese authorities, came to S’pore in 2021.

An executive at a remote lottery business operating from the Philippines and Cambodia, and targeting gamblers from China

Term: 13 months

Name: Su Haijin

Age: 41

Nationality: Originally from China, holds Cyprus and Vanuatu passports

Charges: 14

Term: 14 months

# Designated Non-Financial Businesses and Professionals

Lawyers
Real Estate
Accountants
Follow Luke Raven for more AML Memes

What other DNFBPs can you think of?

INTERNAL. This information is accessible to ADB Management and staff. It may be shared outside ADB with appropriate permission.

# Importance of transaction monitoring

- Transaction monitoring (TM) is a key control in financial institutions' (FIs) AML/CFT policies and procedures
- An effective TM system enables FIs to detect and assess whether customers' transactions pose suspicion when considered against their respective backgrounds and profiles
- TM systems also facilitate holistic reviews of customer transactions over periods of time, in order to monitor for any unusual or suspicious trends, patterns or activities that may take place

# Transaction monitoring process chain

- Risk assessment
- Customer due diligence

- Parameter, threshold and scenario setting
- Back testing
- Data integrity

- Pre-transaction checks
- Alert handling
- Documentation

- STR filing
- Post STR practices
- Quality assurance and system refinements

# Examples of scenarios to monitor transactions

The number of alerts generated within each bank varies based on several factors, including the number of transactions running through the monitoring system, as well as the rules and thresholds the bank employs within the system to generate the alerts. Banks typically score alerts based on elements contained in the alert, which determines the alert's priority.

Some typical scenarios:

- Large or complex transactions with no visible/apparent economic reasons
- Deposit or transfer of funds without any specific justification
- Frequent cross-border flow of transactions, especially with high-risk countries/geographies
- Aggregated frequent and small transactions
- Unusual patterns of physical cash deposits or withdrawals, which are large when aggregated over a period
- Transaction inconsistent with customer's business profile
- Payment received in account, not matched with goods shipped
- Significant deviations from past account activity
- The sudden large deposit in the dormant accounts
- Detection of activities or behaviors consistent with certain predicate offences (e.g., possible tax evasion or avoidance, corruption nexus, or terrorism financing)

Forced labour can be understood as work that is performed **involuntarily** and **under the menace of any penalty**. It refers to situations in which persons are coerced to work through the use of violence or intimidation, or by more subtle means such as manipulated debt, retention of identity papers or threats of denunciation to immigration authorities.

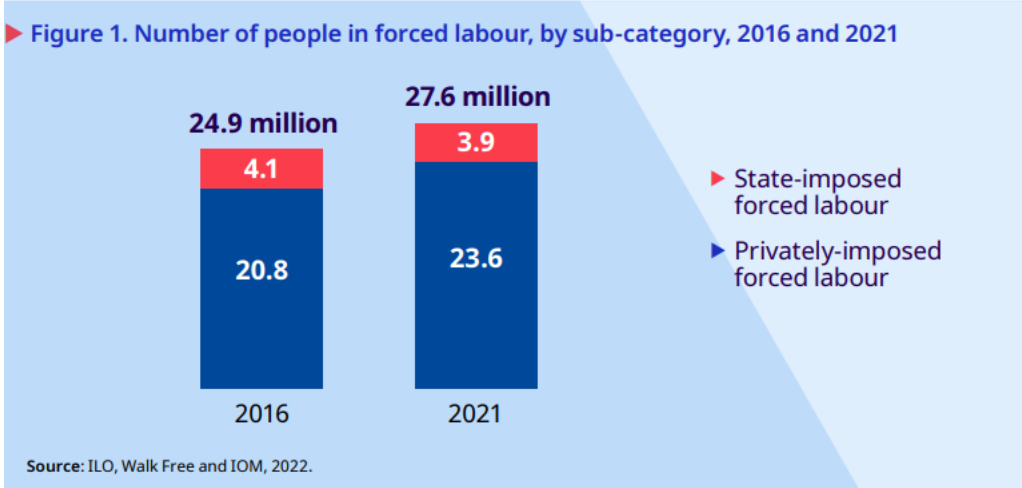
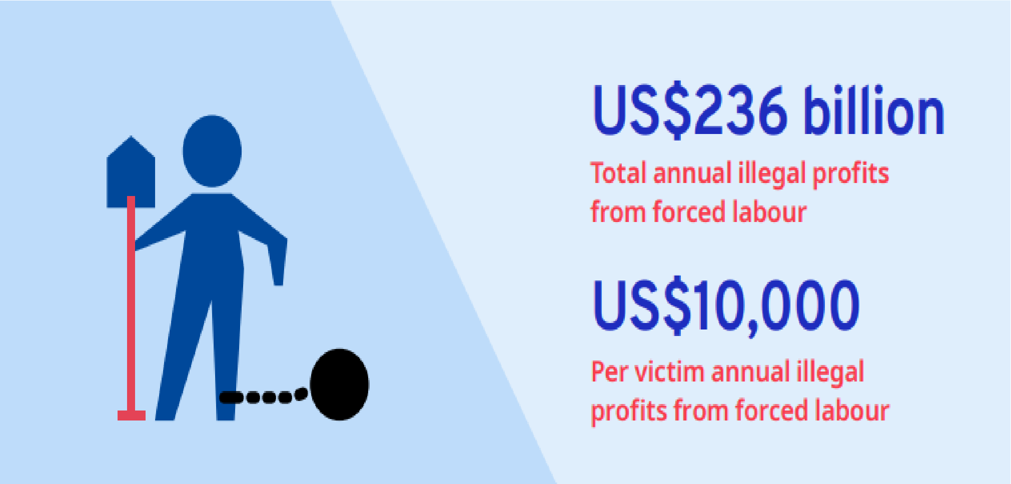


Figure 1. Number of people in forced labour, by sub-category, 2016 and 2021

**Source:** ILO, Walk Free and IOM, 2022.


**US$236 billion**

Total annual illegal profits from forced labour

**US$10,000**

Per victim annual illegal profits from forced labour

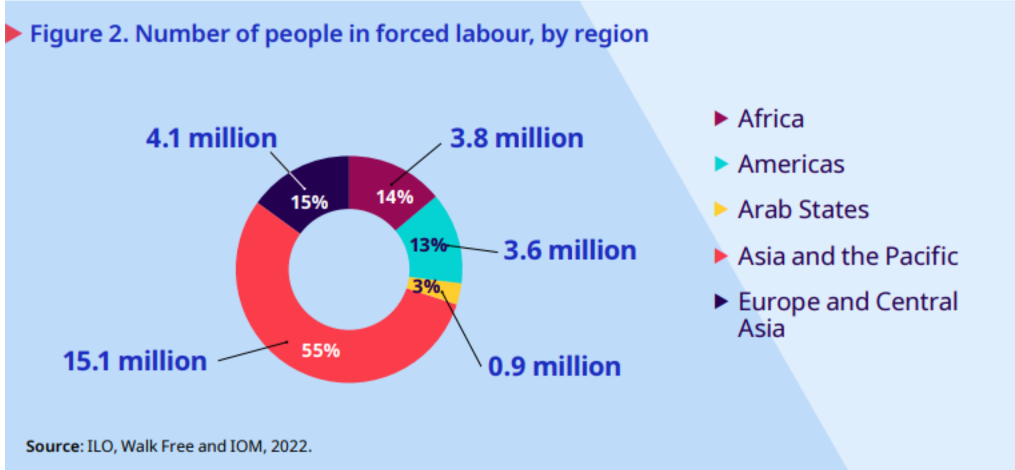


Figure 2. Number of people in forced labour, by region

**Source:** ILO, Walk Free and IOM, 2022.

Source: ILO Profits and poverty: The economics of forced labour report March 2024

Police in Singapore, Hong Kong and South Korea have arrested 272 people in a joint operation targeting child pornography and sexual exploitation.

The suspects, aged between 12 and 73, were arrested during a five-week operation from Feb 26 to Mar 29, during which authorities raided a total of 236 locations.

# Discuss

**Imagine yourselves working in a financial institution**

What would be the scenarios you can build in the transaction monitoring systems to detect potential OSEC?*

What are the considerations?

* *Online Sexual Exploitation of Children*

## When the payments stop, so will the abuse …

***Eric Favila***
*Founder & CEO*
*AMLakas Corporation*

# A Tale of the Baker and the Banker

# The 24-Hour Florist

# What we need

# Effective transaction monitoring system

An effective TM system is comprised of the following elements.

- A well-calibrated framework
- Robust risk awareness
- Meaningful integration
- Active oversight

# Good practice

## Examples of good practice

- The firm has considered what mixture of manual and automated screening is most appropriate.
- There are quality control checks over manual screening.
- Where a firm uses automated systems, these can make ‘fuzzy matches’ (e.g., able to identify similar or variant spellings of names, name reversal, digit rotation, character manipulation, etc.).
- The firm screens customer directors and known beneficial owners on a risk-sensitive basis.
- Where the firm maintains an account for a listed individual, the status of this account is clearly flagged to staff.
- A firm only places faith in other firms’ screening (such as outsourcers or intermediaries) after taking steps to satisfy themselves this is appropriate.

# Poor practice

**Examples**

- The firm assumes that an intermediary has screened a customer but does not check this.
- Where a firm uses automated systems, it does not understand how to calibrate them and does not check whether the number of hits is unexpectedly high or low.
- Screening of customer databases is a one-off exercise.
- Updating from the consolidated list is haphazard.
- Some business units use out-of-date lists.
- The firm has no means of monitoring payment instructions.

# Artificial Intelligence (“AI”) and Machine Learning (“ML”)

- Ability to analyze vast amounts of data quickly and accurately
- Can identify patterns and anomalies that may go unnoticed by manual processes
- By utilizing natural language processing, machine learning, and pattern recognition, AI-powered systems can train models on huge volumes of consumer behavior data they generate to learn fraud patterns and to then detect fraudulent behavior, transactional patterns and financial networks
- Allows compliance teams to focus their efforts on analyzing high-risk cases, rather than sifting through vast amounts of data manually
- Ensures a consistent and standardized approach to AML compliance

# Challenges and considerations of using AI/ML

The need to ensure data integrity, privacy, and regulatory compliance throughout the process

- Data quality and integrity - AI models heavily rely on accurate and reliable data
- Data privacy and maintaining explainability in AI algorithms - ensure compliance with data protection regulations and maintain transparency in their AI models to gain trust from regulators and stakeholders
- Ongoing monitoring and validation of AI models to ensure their effectiveness and accuracy

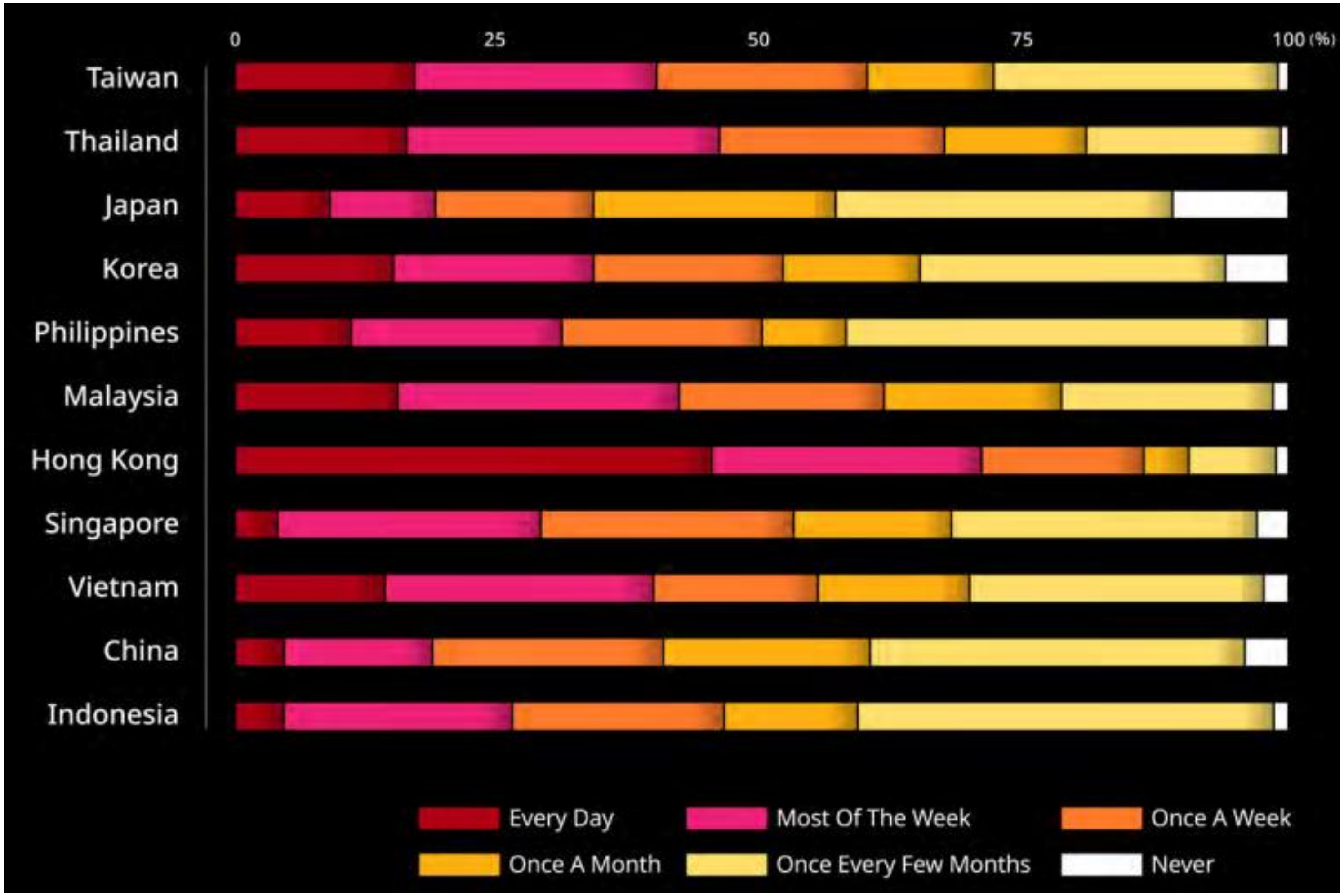
# Will Artificial Intelligence ("AI") take over our jobs?

AI is neither "Artificial" nor "Intelligent" – Kate Crawford, Microsoft

AI is built with "natural resources and it is people who are performing the tasks to make the systems appear autonomous."

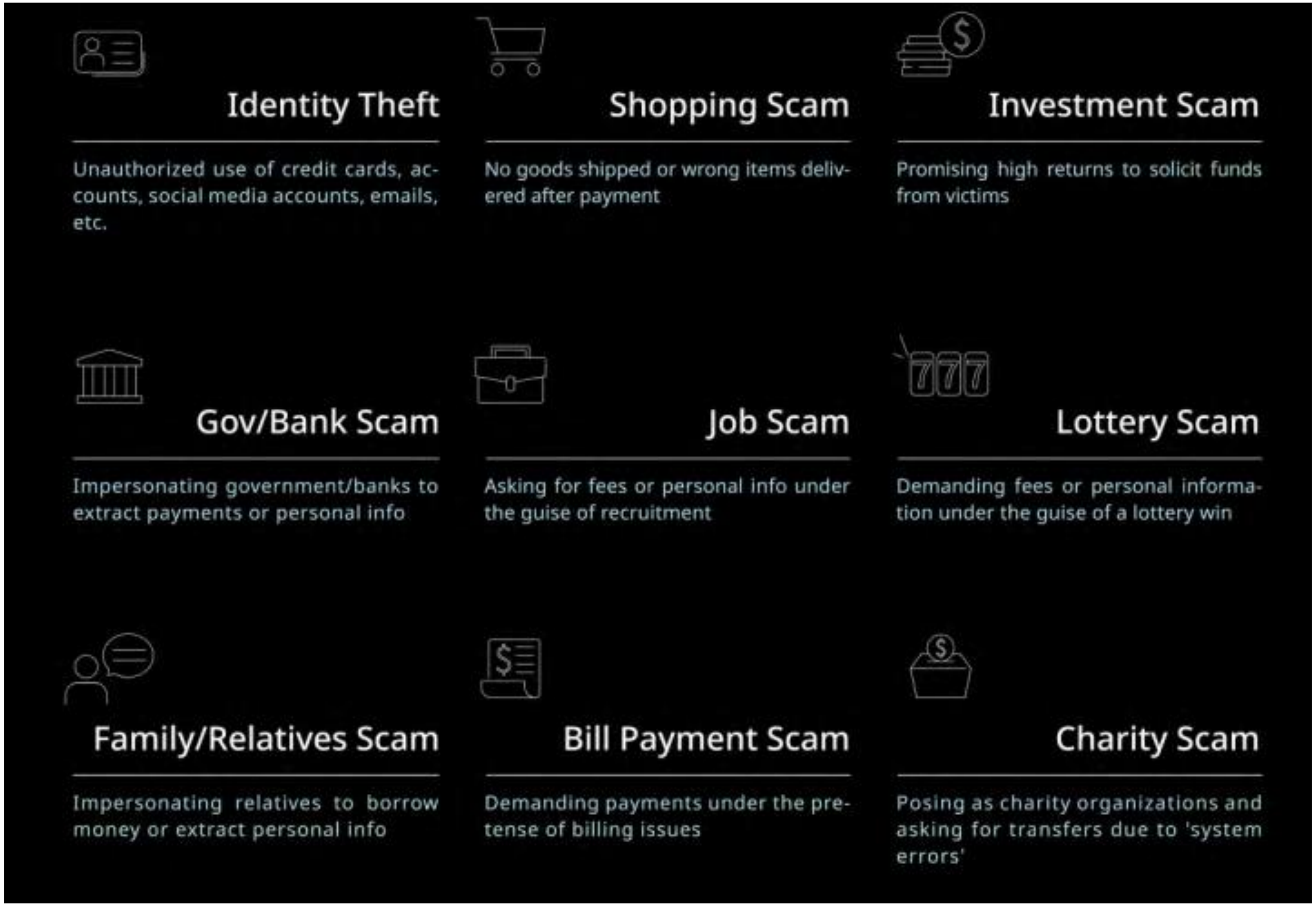
# My Story

# Frequency of Encountering Scams



Source: 2023 Asia Scam Report

# Scam Scenarios and Techniques



### Identity Theft

Unauthorized use of credit cards, accounts, social media accounts, emails, etc.

### Shopping Scam

No goods shipped or wrong items delivered after payment

### Investment Scam

Promising high returns to solicit funds from victims

### Gov/Bank Scam

Impersonating government/banks to extract payments or personal info

### Job Scam

Asking for fees or personal info under the guise of recruitment

### Lottery Scam

Demanding fees or personal information under the guise of a lottery win

### Family/Relatives Scam

Impersonating relatives to borrow money or extract personal info

### Bill Payment Scam

Demanding payments under the pretense of billing issues

### Charity Scam

Posing as charity organizations and asking for transfers due to 'system errors'

Source: 2023 Asia Scam Report

# What is Social Engineering?

Technique used by attackers to manipulate individuals into divulging confidential information, performing actions, or compromising security measures.

Social engineering relies on exploiting human psychology and behavior.

**Phishing**: Sending deceptive emails or messages pretending to be from a trusted source, such as a bank or a colleague, in order to trick recipients into revealing sensitive information like passwords or credit card numbers

**Pretexting**: Creating a fabricated scenario or pretext to manipulate individuals into disclosing information or performing actions they normally would not

**Baiting**: Offering something enticing, such as a free download (e.g. Android Package Kit), that contains malware, with the aim of infecting the victim’s device

**Quid pro quo**: Offering a service or benefit in exchange for sensitive information

**Impersonation**: Pretending to be someone else, either in person, over the phone, or online, in order to gain access to restricted areas or information

# Keeping up with times

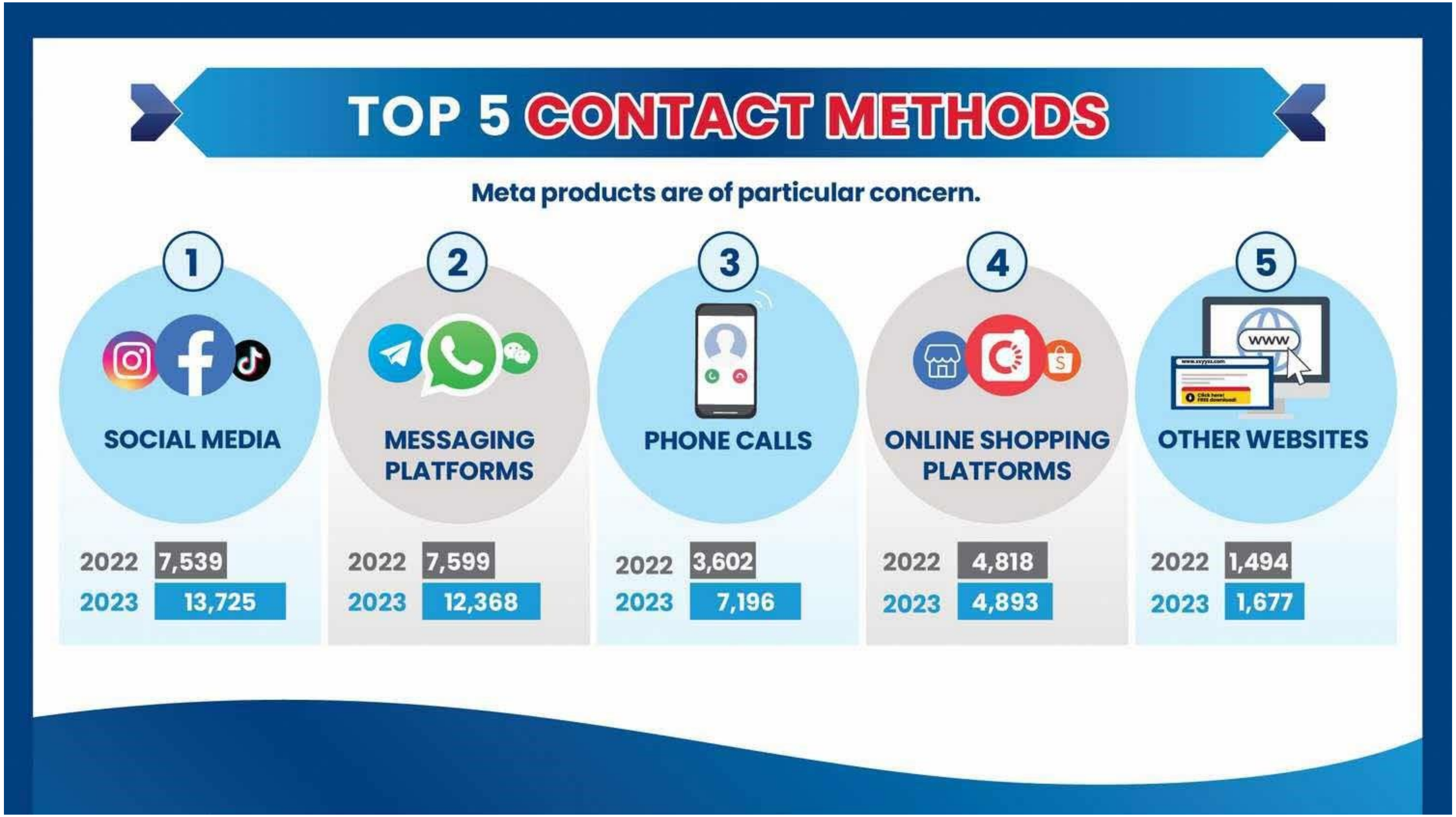
Phishing or pressure received unsolicited via social media, emails, SMSes, phone calls

Promises of lottery winning or great returns

Appeals to the heart e.g. romance, charity or supporting loved ones

Threats to harm financially, socially, physically or legally

# Fraud and Scams in Singapore



## TOP 5 CONTACT METHODS

Meta products are of particular concern.

| | 1 SOCIAL MEDIA | 2 MESSAGING PLATFORMS | 3 PHONE CALLS | 4 ONLINE SHOPPING PLATFORMS | 5 OTHER WEBSITES |
|---|---|---|---|---|---|
| 2022 | 7,539 | 7,599 | 3,602 | 4,818 | 1,494 |
| 2023 | 13,725 | 12,368 | 7,196 | 4,893 | 1,677 |

Source: Singapore Annual Scams and Cyber Crime Report 2023

INTERNAL. This information is accessible to ADB Management and staff. It may be shared outside ADB with appropriate permission.

# On Fraud and Scams

**Unity is the ultimate key to combat fraud – Jackie Cheng, GASA Director of Board and Gogolook Chair**

# Compliance does not stop Financial Crime, People do

# Preliminary Survey - top questions/main concerns do you have with regards to Financial Crime Compliance and/or Correspondent Banking?

| | | |
|---|---|---|
| 1. | Digital technology | |
| 2. | How to identify, detect and prevent fraud and scams | ✹ |
| 3. | Applying best practices over conducting due diligence checks and not over checking. | ✹ |
| 4. | What are the types of risks associated with the correspondent banking and how do we mitigate the risks? | ✹ |
| 5. | Sanctions exposure | ✹ |
| 6. | From a correspondent bank's perspective, main concern is on nested payment intermediary (PI) relationship as Banks and PIs may not be subjected to the same level of regulatory scrutiny. Banks will need to scrutinise and monitor more complicated scenarios for nesting involving combination of respondent bank and their Bank customer or PI customers or even another level down. | ✹ |
| 7. | Correspondent banking CDDs will need to factor in more vostro review and understanding the proper application of the MX SWIFT messages to develop proper tools to identify for correspondent banking monitoring. Traditional review of CBDDQ and questionnaire may be rendered inadequate for risk management especially when providing Vostro accounts. | |

# Preliminary Survey - top questions/main concerns do you have with regards to Financial Crime Compliance and/or Correspondent Banking?

| | | |
|---|---|---|
| 8. | Despite they have policies and procedures, what is the comfort level if they are abiding by it | ✹ |
| 9. | Do we have a robust core banking system, adequate controls and measures for anti-financial crime? | ✹ |
| 10. | How to address the underlying concerns of OFAC, FDIC and FED to create a correspondent banking model that meets the needs of Asian (and African) banks who have been systemically disenfranchised (de-risked) by US Banks - either directly or through their regional counterparties. | ✹ |
| 11. | In our quest to find a solution to the CBR problem and given the complexity of it, how do we break it down into smaller actionable steps for the Pacific Island Countries | |
| 12. | The lack of harmonization of different domestic laws and policies | |
| 13. | What the reason and why derisking of banks in the Pacific. | ✹ |
| 14. | A country's correspondent banking relationships with other jurisdictions | |
| 15. | Compliance is a moving target | ✹ |

# Preliminary Survey - top questions/main concerns do you have with regards to Financial Crime Compliance and/or Correspondent Banking?

| | | |
|---|---|---|
| 16. | Rising cost of compliance | ✹ |
| 17. | What role can partner Governments' play to improve financial crime compliance and support an ongoing correspondent banking presence in the Pacific | ✹ |
| 18. | What AI tools are available to assist business and agencies dealing with aspects of FCC | ✹ |
| 19. | Trade Base Money Laundering-lack of understanding | ✹ |
| 20. | How do we ensure financial crime is not facilitated through block chain, smart contracts, and distributed ledgers | ✹ |
| 21. | Customer due diligence conducted by correspondent banks | ✹ |
| 22. | Current regulations | |
| 23. | Areas where risk to correspondent banking can be misused by criminals? | ✹ |
| 24. | Exploiting the banking system to layer funds related to money laundering investigations. | |

# Questions?

# Have Burning Questions?

https://app.sli.do/event/cUwyq4kBsmG5JqHhxzhWpR

Join at slido.com: #2286357

(live until 11 April 2024)

# Thank you.

# Resources

- ILO Profits and poverty: The economics of forced labour report March 2024: https://www.ilo.org/global/topics/forced-labour/publications/WCMS_918034/lang--en/index.htm
- Police in Singapore, Hong Kong and South Korea arrest 272 suspects in joint operation targeting chil porn: Police in Singapore, Hong Kong and South Korea arrest 272 suspects in joint operation targeting child porn - CNA (channelnewsasia.com)
- Singapore Annual Scams and Cybercrime report 2023: https://www.police.gov.sg/Media-Room/Police-Life/2024/02/Three-Things-you-Should-Know-About-the-Annual-Scams-and-Cybercrime-Brief-2023
- 2023 Asia Scam Report: https://files.gogolook.com/2023-asia-scam-report