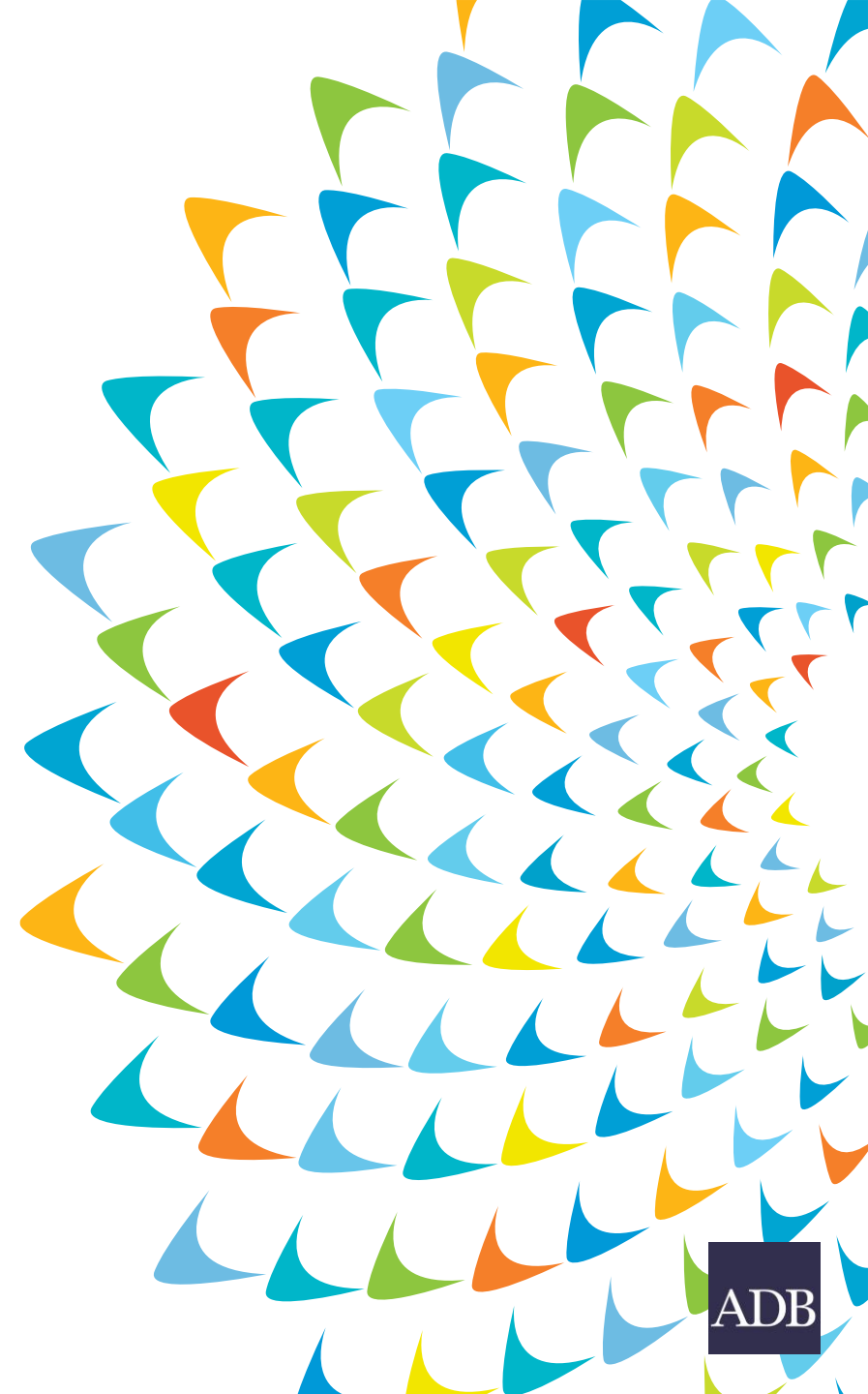


The views expressed in this presentation are the views of the author/s and do not necessarily reflect the views or policies of the Asian Development Bank, or its Board of Governors, or the governments they represent. ADB does not guarantee the accuracy of the data included in this presentation and accepts no responsibility for any consequence of their use. The countries listed in this presentation do not imply any view on ADB's part as to sovereignty or independent status or necessarily conform to ADB's terminology.

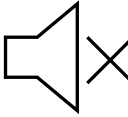
Enterprise-Wide Risk Assessment

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/tcMSXNhrNrKLiP7yZzh43D>

Join at [slido.com](https://www.slido.com/join/#2286357): #2286357
(live until 5 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 3



FATF Recommendations 5,6,7 and 8

5. Terrorist Financing Offence - to criminalize terrorist financing on the basis of the Terrorist Financing Convention, and should criminalize not only the financing of terrorist acts but also the financing of terrorist organizations and individual terrorists even in the absence of a link to a specific terrorist act or acts
6. Targeted financial sanctions related to terrorism and terrorist financing
7. Targeted financial sanctions related to proliferation
8. Non-profit organizations - identify the organizations which fall within the FATF definition of non-profit organizations (NPOs) and assess their terrorist financing risks, in line with risk based approach



FATF Effectiveness – Immediate Outcomes



- 1 | Risk, Policy and Coordination**
Money laundering and terrorist financing risks are understood and, where appropriate, actions coordinated domestically to combat money laundering and the financing of terrorism and proliferation.
- 2 | International cooperation**
International cooperation delivers appropriate information, financial intelligence, and evidence, and facilitates action against criminals and their assets.



- 3 | Supervision**
Supervisors appropriately supervise, monitor and regulate financial institutions and DNFBPs for compliance with AML/CFT requirements commensurate with their risks
- 4 | Preventive measures**
Financial institutions and DNFBPs adequately apply AML/CFT preventive measures commensurate with their risks, and report suspicious transactions.
- 5 | Legal persons and arrangements**
Legal persons and arrangements are prevented from misuse for money laundering or terrorist financing, and information on their beneficial ownership is available to competent authorities without impediments

- 6 | Financial intelligence**
Financial intelligence and all other relevant information are appropriately used by competent authorities for money laundering and terrorist financing investigations.

- 7 | Money laundering investigation & prosecution**
Money laundering offences and activities are investigated and offenders are prosecuted and subject to effective, proportionate and dissuasive sanctions.

- 8 | Confiscation**
Proceeds and instrumentalities of crime are confiscated.

- 9 | Terrorist financing investigation & prosecution**
Terrorist financing offences and activities are investigated and persons who finance terrorism are prosecuted and subject to effective, proportionate and dissuasive sanctions.



- 10 | Terrorist financing preventive measures & financial sanctions**
Terrorists, terrorist organisations and terrorist financiers are prevented from raising, moving and using funds, and from abusing the NPO sector.
- 11 | Proliferation financial sanctions**
Persons and entities involved in the proliferation of weapons of mass destruction are prevented from raising, moving and using funds, consistent with the relevant UNSCRs.

Source: <https://www.fatf-gafi.org/en/publications/Fatfgeneral/Effectiveness.html>



High-Risk Jurisdictions subject to a Call for Action - Feb 2024 aka FATF Black List



Democratic People's Republic of Korea



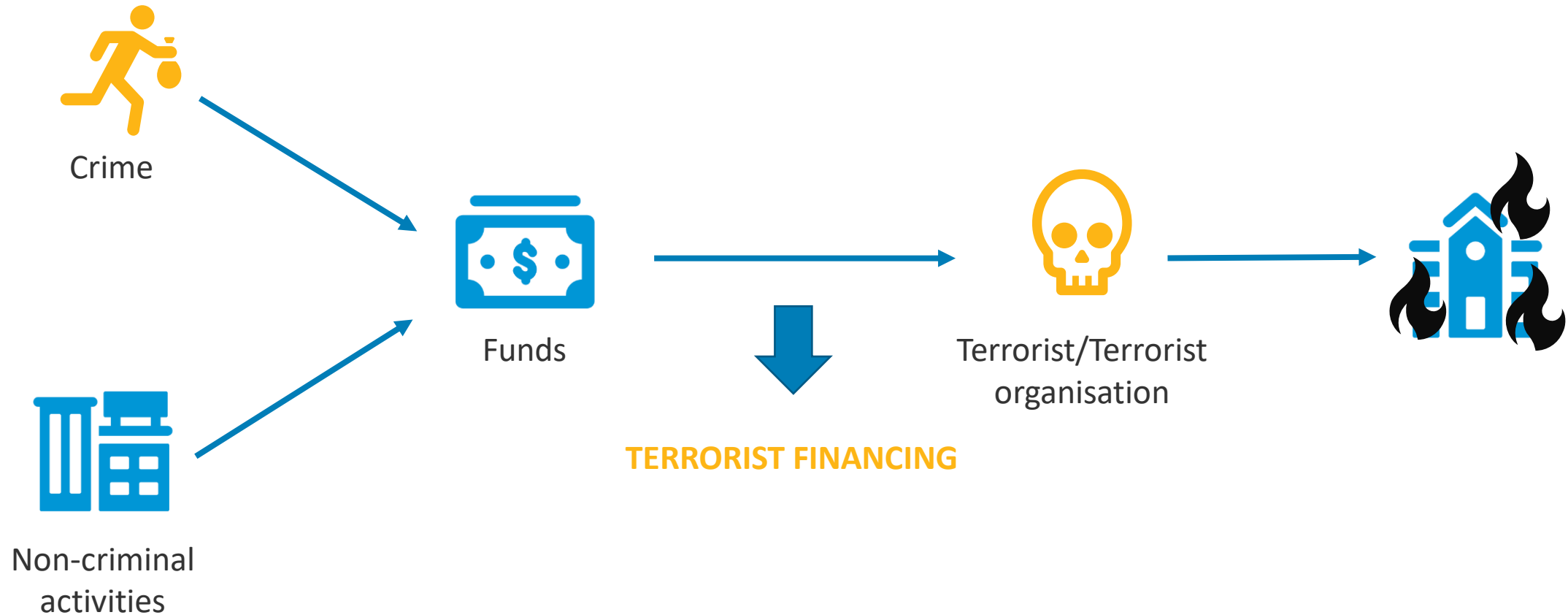
Iran



Myanmar



Terrorist Financing





FATF - Proliferation financing

Refers to the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery and related materials including both technologies and dual use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations



Nature and Types of Sanctions

Nature of sanction

1. Comprehensive
2. Country / Regime-based
3. Activity-based

Types of sanction

1. Financial Sanctions
2. Economic Sanctions
3. Trade Sanctions
4. Other Sanctions



Sanctions

- Restrictions imposed against an individual, entity or country
- Imposed by governments or intergovernmental bodies (e.g., UNSC or OFAC)
- Example of sanctions
 - Economic, Diplomatic, Trade, Individual, Vessels
 - Administered for the purpose of combatting terrorism, terrorist financing, proliferation and proliferation financing (dealing with weapons of mass destruction (WMDs))

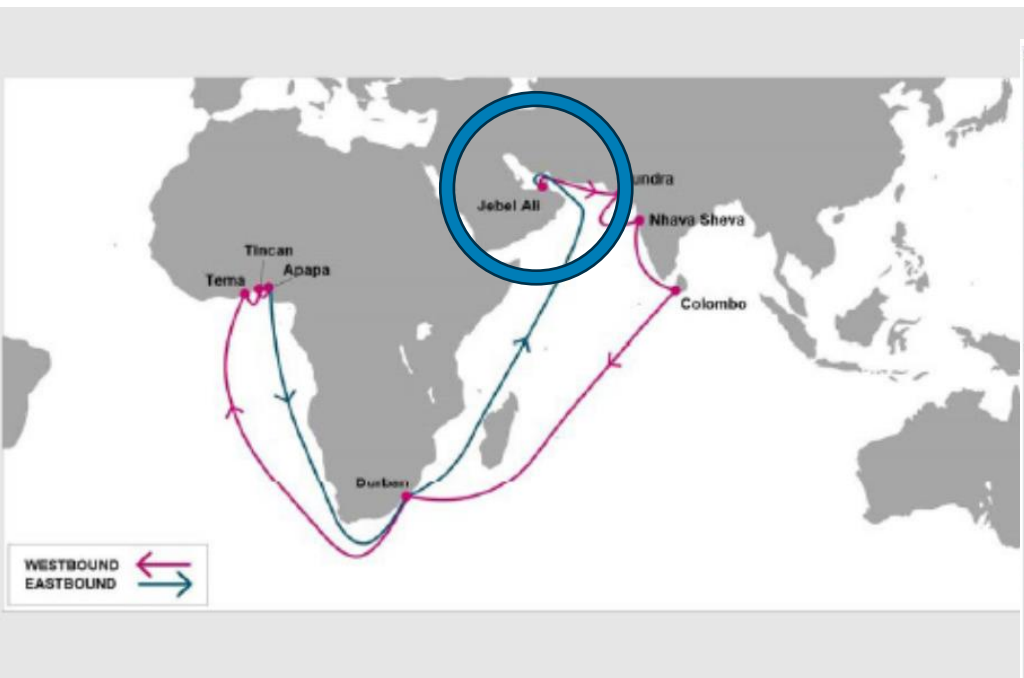


US office of foreign assets control (OFAC)

- Administers and enforces economic and trade sanctions based on US foreign policy and national security goals
- Sanctions include:
 - targeted foreign countries and regimes
 - terrorists
 - international narcotics traffickers
 - those engaged in activities related to the proliferation of weapons of mass destruction and
 - any other threats to the national security, foreign policy or economy of the US



Practical aspects - Trade



No Shipping = No Shopping



Trade-Based Money Laundering (“TBML”)

Common red flags:

- Over- or Under-invoicing: Significant discrepancies between the stated value of goods on invoices and their actual market value
- Multiple Invoicing: Involves generating multiple invoices for the same transaction, often with varying amounts
- Misrepresentation of Goods: The description of goods on shipping documents or invoices does not match the actual goods being shipped.
- High-Risk Products or Industries: Certain goods or industries are more susceptible to TBML due to their complexity, high value, or ease of manipulation (e.g., electronics, precious metals, pharmaceuticals).
- Unusual Shipping Routes or Methods: Transactions involving circuitous shipping routes or unconventional shipping methods
- Cash Payments in International Trade: Payments made in cash for international trade transactions, especially in large amounts, can indicate attempts to conceal the true source
- Third-Party/Unrelated parties Payments: Payments to or from third parties not directly involved in the transaction, particularly in high-risk jurisdictions or with a history of financial crime, or Entities with no apparent business relationship engaging in trade transactions.
- Shell Companies or Fronts: Utilization of shell companies or front companies to obscure the beneficial ownership of assets involved in trade transactions.
- Round-Trip Transactions: Transactions where goods are sold and then repurchased by the same party, often in a different jurisdiction, without a legitimate economic purpose.
- Freight Forwarding Anomalies: Abnormalities in freight forwarding practices, such as frequent changes in freight forwarders or using unregistered freight forwarders.



Dual use goods

Dual-use goods refer to items, materials, or technologies that can have both civilian and military applications:

Advanced Materials: Materials such as carbon fiber, advanced ceramics, and certain polymers can be used in civilian applications like sports equipment or aerospace components, but they also have military applications in armor, missile components, or aircraft structures

Electronics: High-performance electronics like microprocessors, integrated circuits, and sensors can be used in consumer electronics, telecommunications, or medical devices, but they also have military applications in surveillance systems, guidance systems, or radar technology

Software and Information Security Tools: Encryption software, cybersecurity tools, and communication protocols can have both civilian and military uses. While they are essential for securing sensitive information in banking, e-commerce, and communications, they are also vital for military communications and securing classified data

Chemicals and Pharmaceuticals: Certain chemicals and pharmaceuticals can have both civilian and military applications. For example, chemicals used in agricultural fertilizers or pharmaceuticals used in medical treatments can also be used in the production of chemical weapons or in military medical facilities

Aerospace Technologies: Technologies developed for civilian aerospace purposes, such as satellite technology, remote sensing, or navigation systems (like GPS), also have significant military applications in reconnaissance, surveillance, and precision-guided munitions



Dual use goods

Machine Tools and Manufacturing Equipment: Advanced machine tools and manufacturing equipment can be used in civilian industries such as automotive or aerospace manufacturing, but they can also be used in the production of military hardware and weapons systems

Nuclear Technology: Nuclear technology has numerous civilian applications, including power generation and medical imaging, but it also has military applications in the development of nuclear weapons and propulsion systems for submarines and aircraft carriers

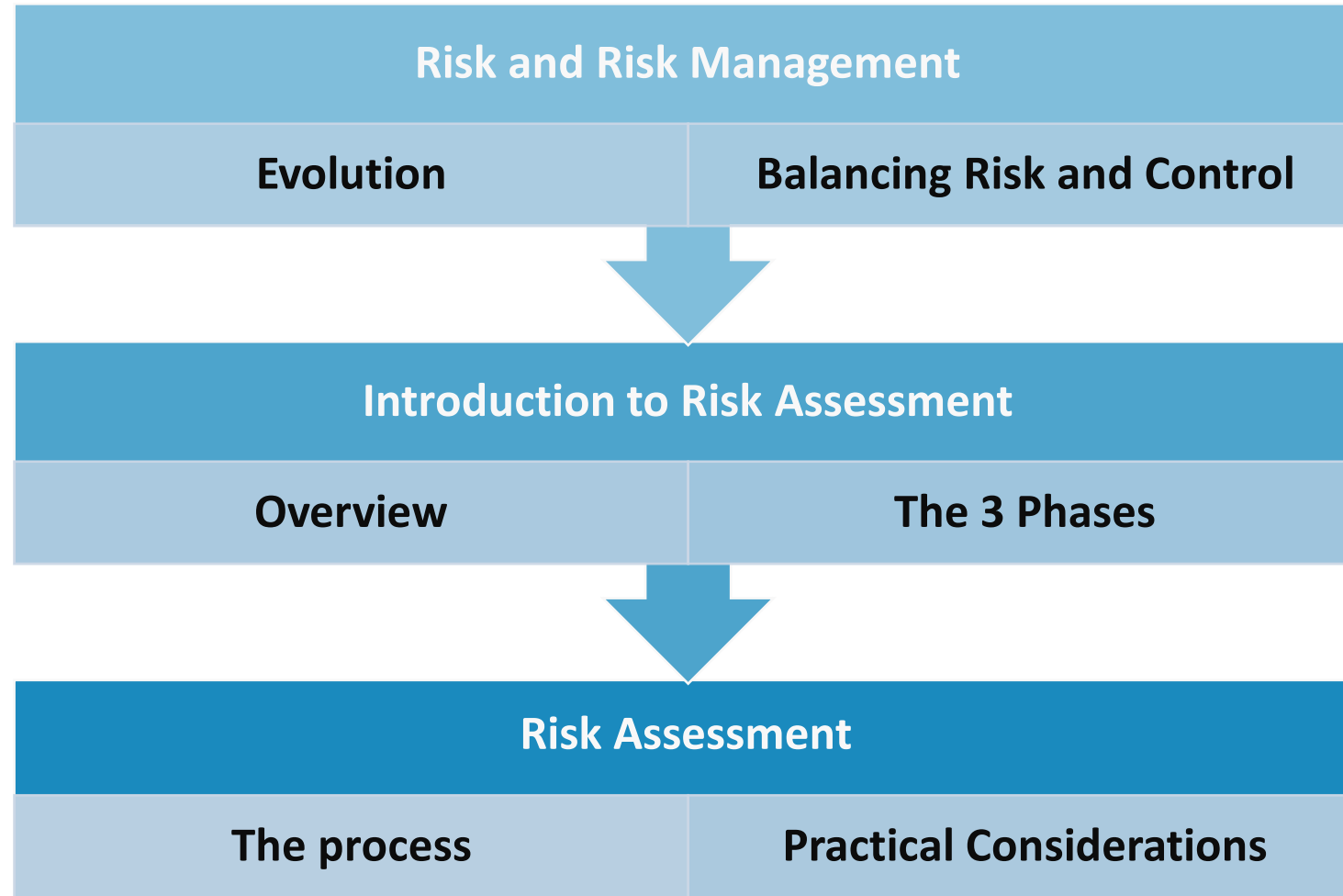
Dual-Use Vehicles and Transportation Equipment: Vehicles and transportation equipment designed for civilian use, such as trucks, aircraft, or ships, can also be adapted for military purposes, such as troop transport, logistics support, or as platforms for weapon systems

Biotechnology: Biotechnology research and products, including genetically modified organisms (GMOs), can have both civilian and military applications. While biotechnology is used in agriculture and medicine, it can also be used in the development of biological weapons or for military medical research

Robotics and Autonomous Systems: Robotics and autonomous systems developed for civilian purposes, such as automated manufacturing or unmanned aerial vehicles (drones) for photography, also have military applications in surveillance, reconnaissance, and even combat operations.



Learning Objectives of this module





**It is almost midnight, the roads are quiet.
The traffic light is showing 'red man'. Would
you cross the road?**

- 1 - Yes
- 2 – No
- 3 – Others (?)

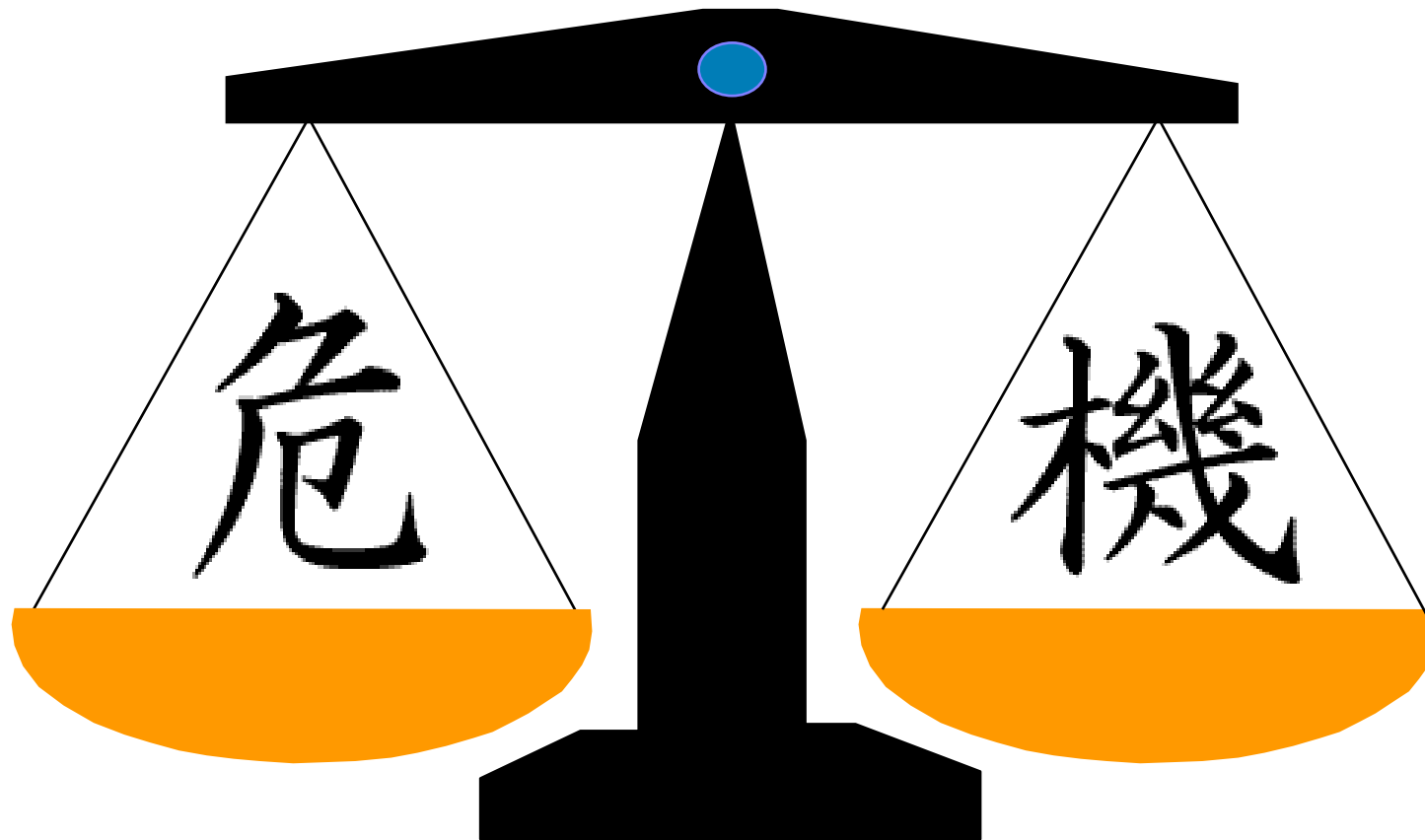
<https://app.sli.do/event/uLpSff9H9LGNTZ2QJZ6TYx>

Join at [slido.com: #7440459](https://www.slido.com/join/#7440459)





Risk Defined





Evolution of Risk Management

Responsibility of Audit



Greater management awareness



Audit cultural revolution



Decision making tool





Evolution of Risk Management – Cont'd

Better Planning / Risk Consideration



Better Decision Making



Audit Revolution

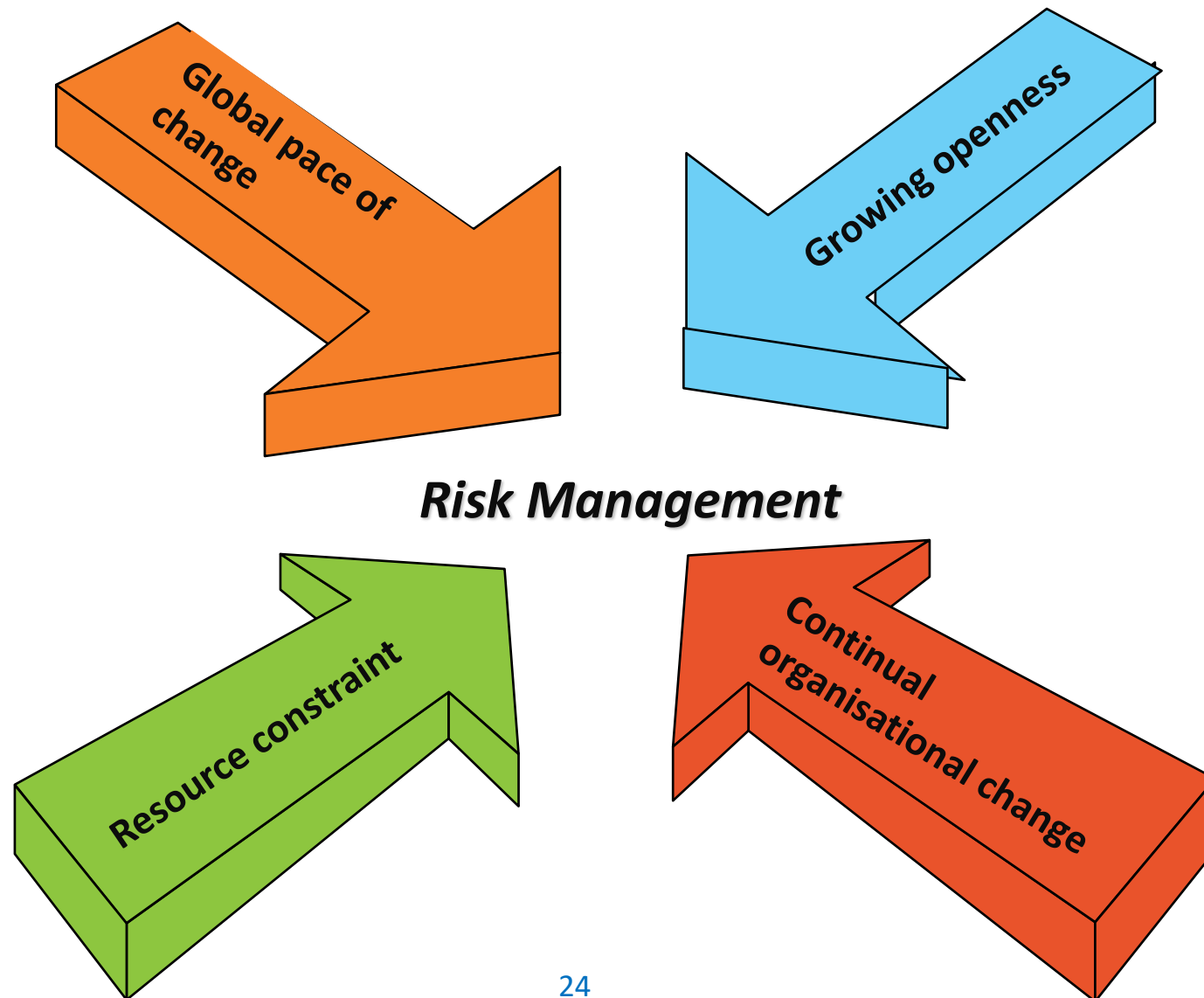


Better Corporate Governance





Factors demanding robust risk management





Factors demanding robust risk management

Any others factors off the top of your minds?



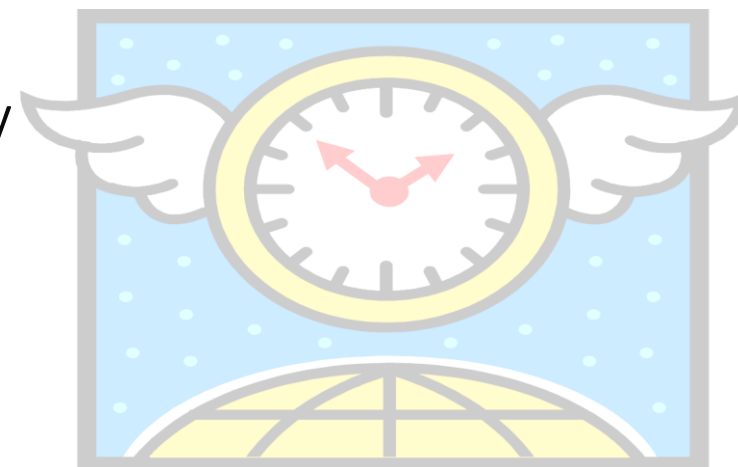
Evolution of Management's View of Risk

From back room ...

- Risk monitoring is a low-level function of the internal auditors
- Risk as a negative opportunity to be controlled
- Risk managed separately in organisational silos
- Responsibility for risk management is delegated to lower levels
- Risk measurement is subjective
- Unstructured and divergent risk management functions

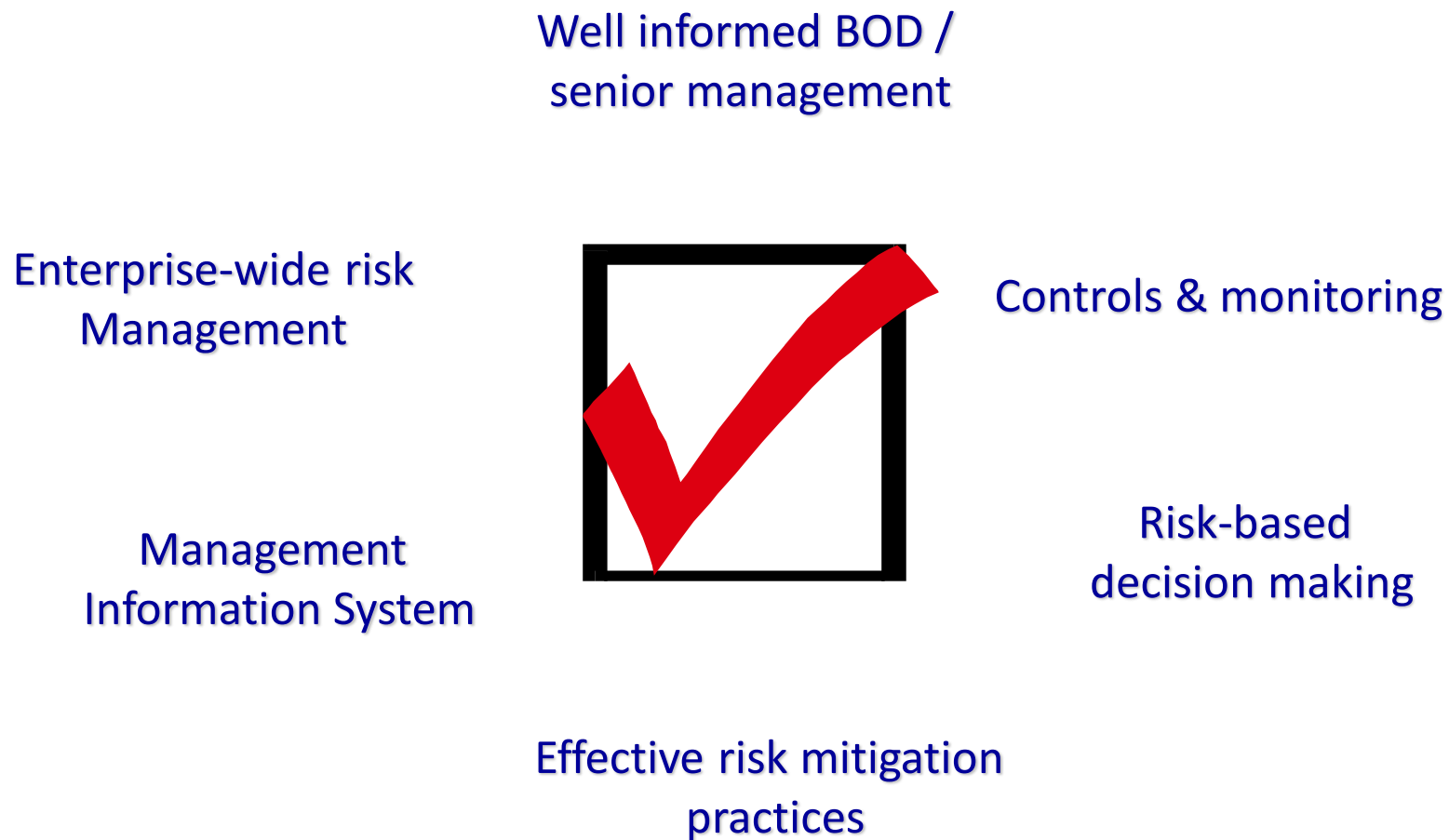
... to board room

- ➔ Risk monitoring is the CEO's job (with board oversight)
- ➔ Risk as an opportunity
- ➔ Risk managed in an integrated, enterprise-wide fashion
- ➔ Risk management is responsibility of senior/line management
- ➔ Quantification of risk
- ➔ Risk management is built into all corporate management systems





What is Sound Risk Management?



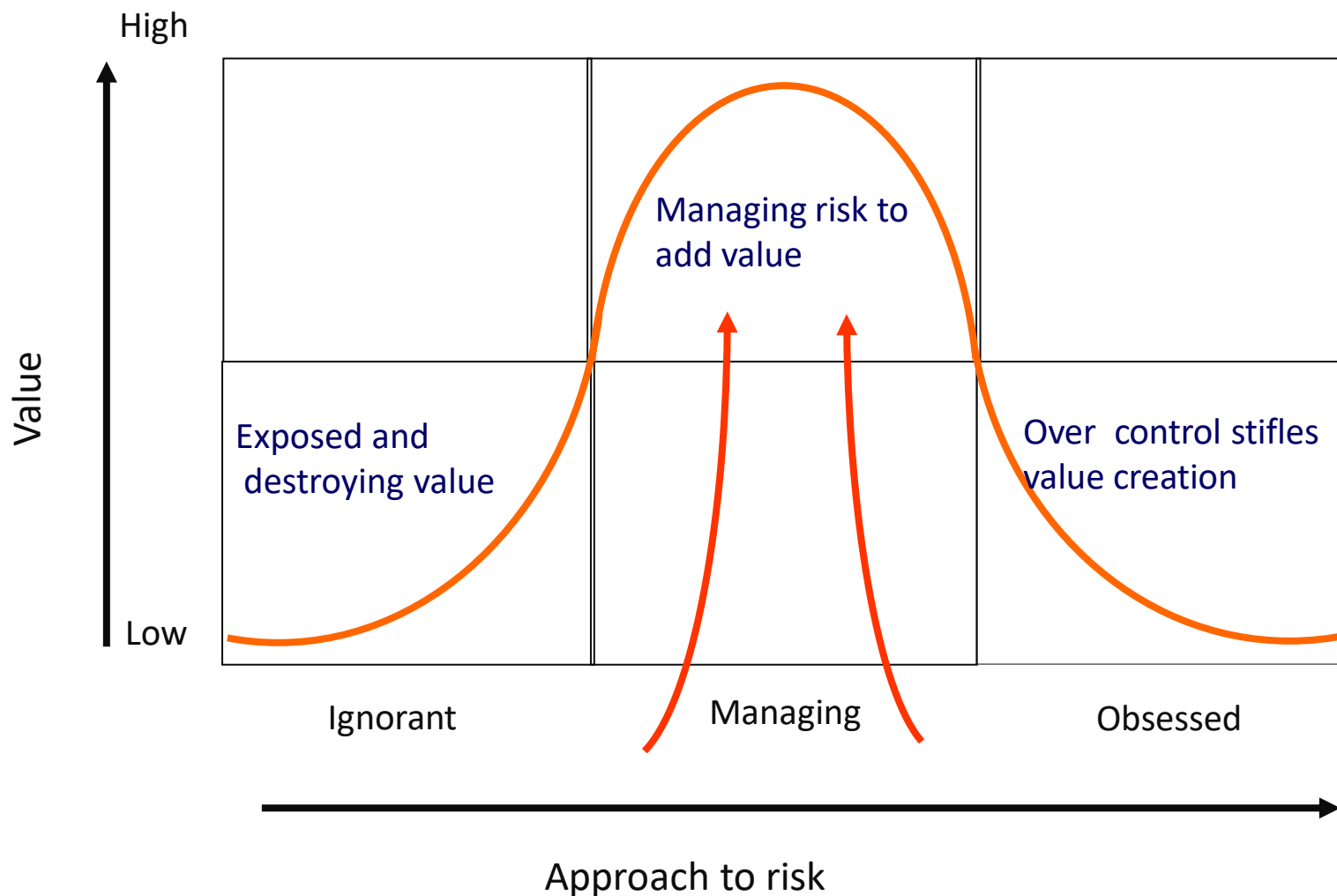


Commercial Drivers for Risk Management





Balancing Risk and Control





Meanwhile, here at home



Zhao Fugang's Yue Lai Hotel, located in Suva, the capital of Fiji.

March 2024:

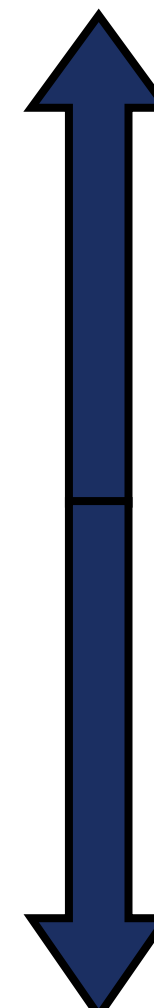
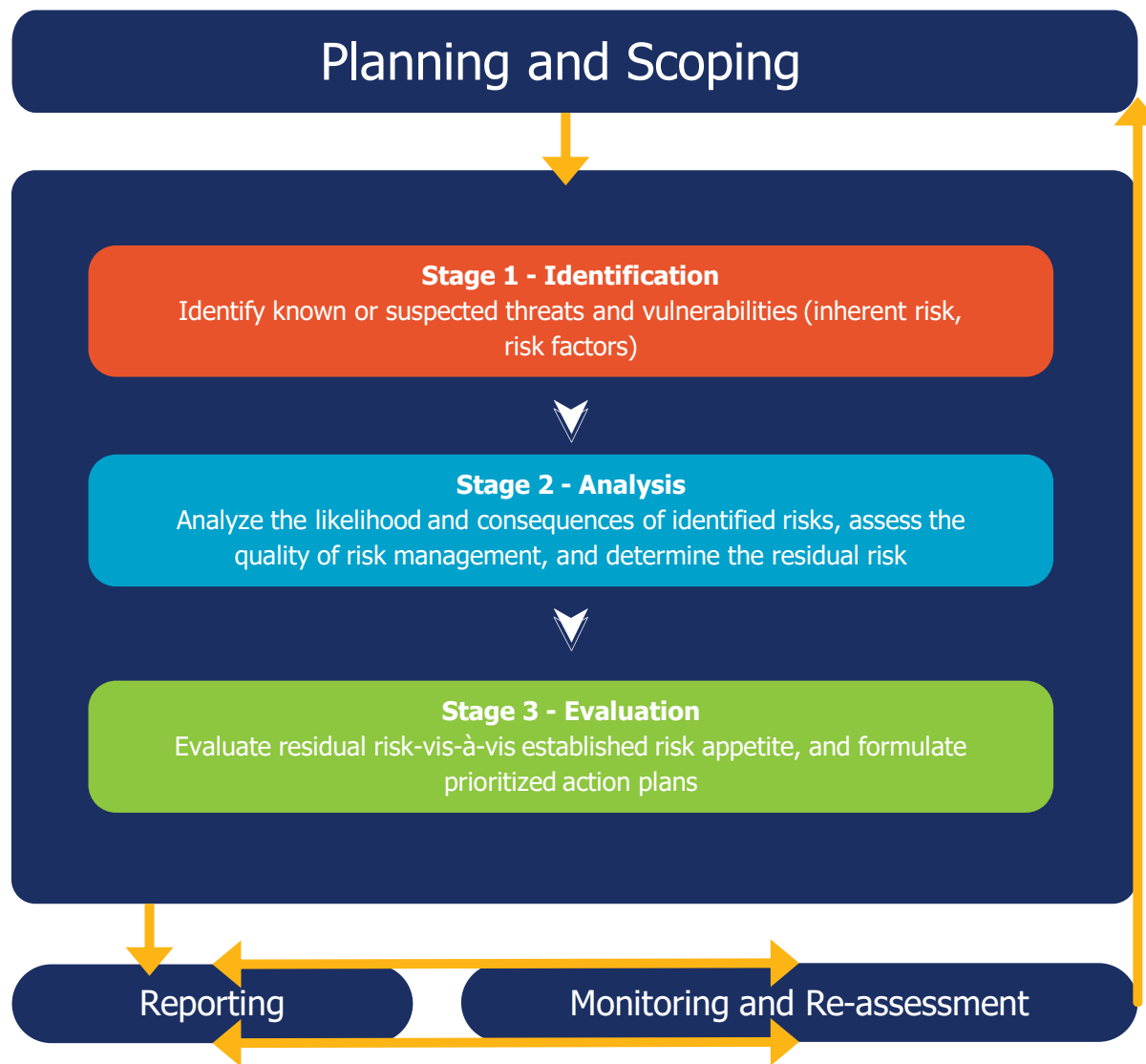
Prominent Fiji-based businessman Zhao Fugang is a trusted advocate for China's interests in the Pacific.

The Australian law enforcement and intelligence agencies suspect he plays another part: as a senior organized crime leader.

Fugang has not been charged with any crime.



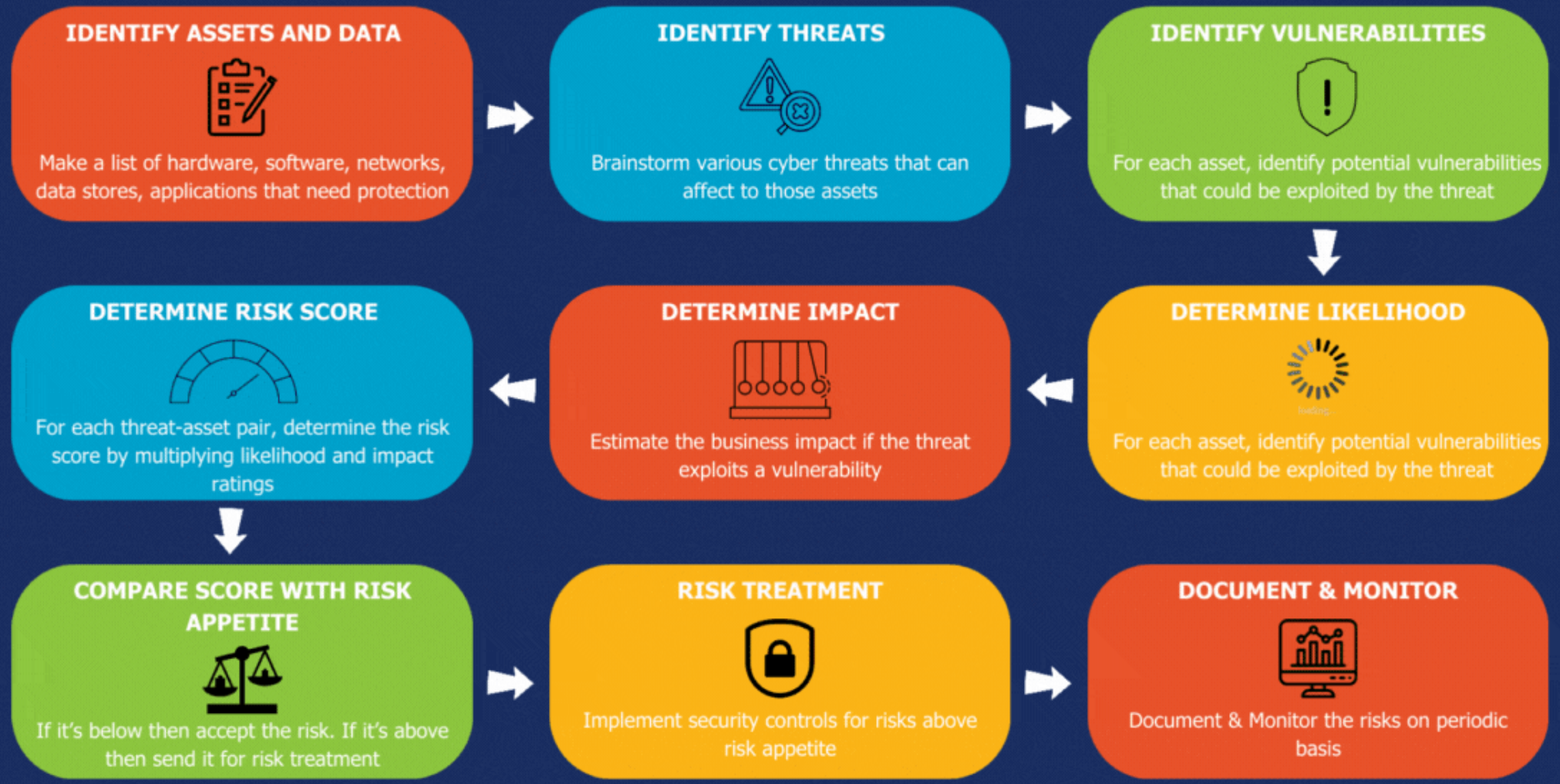
The Risk Assessment Process



EFFICIENT COMMUNICATION



RISK ASSESSMENT PROCESS





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



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



Phase 1 – Inherent Risk Assessment

Inherent Risk represents the exposure to money laundering, sanctions or bribery and corruption risk in the absence of any control environment being applied.

Risk ratings may vary depending upon the size and scope of their businesses and the risks involved. In order to identify an FI's inherent risks, assessment across the following five risk categories is commonly undertaken, although other factors may also be considered:

- Clients (legal entity type, customer's identity, social/financial status, information on nature of business activity and location)
- Products and Services
- Geographies
- Channels
- Other Qualitative Risk Factors





Phase 1 – Inherent Risk Assessment

Ratings

Risk ratings will depend on

- Availability of data with the assessment unit and in internal systems. Where information isn't available (Unknown) such instances may be looked at High Risk
- Banks perception of risk (based on regulatory and internal framework) and
- Risk appetite of the organization

Can be a simple 3 tier rating such as Low, Medium and High depending or 5-tier rating of an additional Low to Moderate and Moderate to High rating.

Impact	High	Medium Risk	High Risk	
	Low	Low Risk	Medium Risk	
	0%	Likelihood		100%

High Risk - There is a high chance of ML/TF/PF occurring in this area, and the impact to the business is high in terms of financial, reputational, or customer impact.

Medium Risk - There is a high chance of ML/TF/PF occurring in this area, but the impact to the business is low, or there is low chance of ML/TF/PF occurring in this area, but the impact to the business, if it will occur, is high.

Low Risk - There is a low chance of ML/TF/PF occurring with little or negligible impact to the business.



Phase 1 – Inherent Risk Assessment

Weights

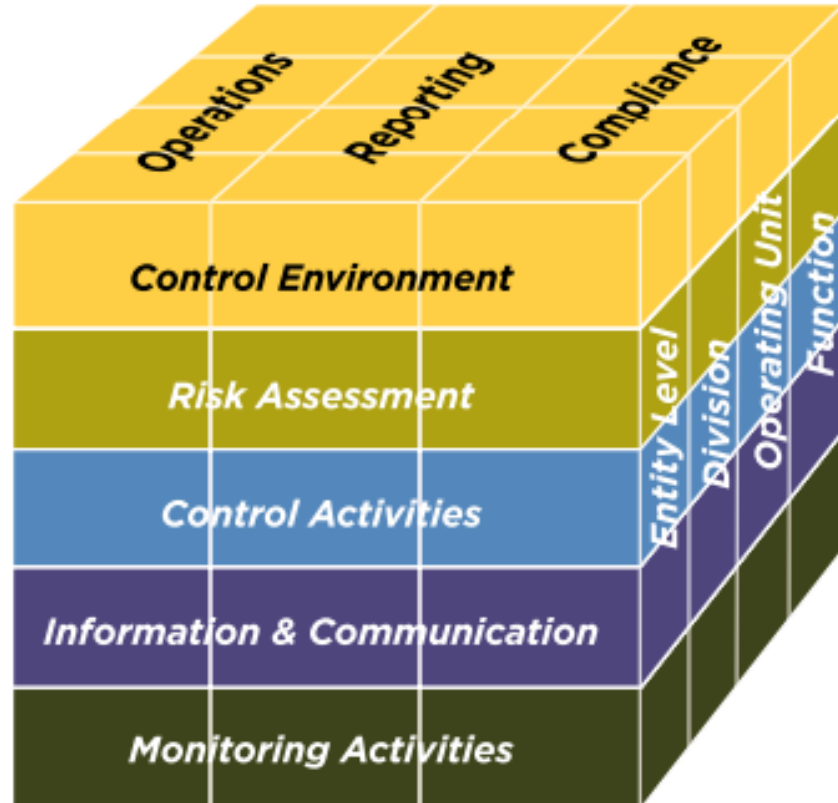
Weight given to each factor is likely to vary from unit to unit, product to product and customer to customer (or even category of customer) and from one FI to another. Factors in determining weighting:

- Not overly influenced by any factor;
- Not influenced by business or profit considerations;
- Not made in such a way that it is impossible for a business to be classified as high risk;
- Assigned weights are not in contravention to regulations and guidelines (national and international)
- Any overrides used should be documented appropriately

Inherent Factor Weighting Examples	
Inherent Factor	Inherent Weighting
Channels	5-10%
Clients	25-35%
Country / Geography	20-30%
Products & Services	20-30%
Other Qualitative Risk Factors	10-15%



Phase 2 – Internal Control Assessment



COSO* – Internal Control Components

* Committee of Sponsoring Organizations- an independent private-sector initiative that studied the causal factors that can lead to fraudulent financial reporting. It also developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.



Phase 2 – Internal Control Assessment

AML controls are usually assessed across the following control categories:

- AML Corporate Governance; Management Oversight and Accountability
- Policies and Procedures
- Know Your Client (“KYC”); CDD, EDD
- Management Information/Reporting
- Monitoring and Controls
- Detection and STR/SAR filing
- Training
- Independent Testing and Oversight (including recent Internal Audit or Other Material Findings)
- Sanctions and screening
- Record Keeping and Retention



Phase 2 – Internal Control Assessment

Weights

As with inherent risk factors, response to each control area is assigned a score, which, when aggregated, reflects the relative strength of that control. Each area can then be assigned a weighting based on the importance that the institution places on that control. For example, CDD may carry a larger weighting than Record Keeping and Retention within risk assessment.

Control Factor Weighting Examples	
Control Factor	Control Weighting
KYC (incl. All requirements)	20-30%
Monitoring & Controls	20-30%
Policies & Procedures	10-15%
Other Risk Assessments	10-15%
AML Corporate Governance; Management Oversight & Accountability	5-10%
Management Information / Reporting	5-10%
Record Keeping & Retention	5-10%
Designated AML Compliance Officer / Unit	5-10%
Detection and SAR Filing	5-10%
Training	5-10%
Independent Testing & Oversight	5-10%
Other Controls / Others	5-10%



Phase 3 – Residual Risk Assessment

Residual Risk is the risk which is the ‘remainder’ risk post assessment of the controls against the identified inherent risks. It represents the ‘balance’ KYC/AML/CFT/Sanctions risk on which controls would have to be built to manage them effectively. The residual risk rating is used to indicate whether the ML risks within the organization are being adequately managed.

Normally residual risk is either denoted on a 3 tier rating scale as Low, Moderate and High Risk or on a 5 tier scale such as Low, Low to Moderate, Moderate, Moderate to High, and High. This would purely depend on the Risk perception of the organization and the depth to which they would like to carry out the Risk assessment and take necessary action.





Risk Assessment Matrix

Inherent Risk Effectiveness Of 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



Reporting and Communicating Results

The results of the ML/CFT risk assessment should be communicated appropriately to the relevant stakeholders. The presentation could be fine tuned to the respective audience. As the output could be voluminous, the help of an internal data analytics team could be taken to make the output easier for consumption . The results can be presented in a number of different ways, highlighting risks by any factors, business division, products, geography or client types etc. This would help the teams to clearly focus on the high risk areas which need immediate attention.

Some of the stakeholders with whom the results can be shared include:

- The Compliance, Risk and Audit departments for necessary post assessment action.
- The Business departments for necessary corrective action.
- Senior management and Board of Directors for information and seeking directives.
- Regulatory and supervisory authorities for guidance.





Monitoring and reassessment

As in every process, the organization has to record a formal process of reassessing the risk identification and mitigation plan, ensure all relevant inherent risks have been covered, whether all existing controls have been defined and recorded for effectiveness and whether the residual risk arising out of the exercise is in line with the normal expectation of the organization. In case of a large variance, the organization may be required to go back to the drawing board to reassess its risk mitigation procedures, controls, policies and procedures etc.

Aspects the firm will need to consider include:

- Changes in products
- New ways of customer onboarding or profiling
- New areas of money laundering being observed based on new typologies released by the regulator or identified internally.
- Introduction of new technology in the area of Risk mitigation.
- Reorientation of staff training and awareness around money laundering/TF
- Strength of control functions in the 2nd / 3rd line of defence including Compliance, Risk and Audit.
- Clear and accurate MIS for decision making by senior management/board



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



- How do we rate our risks?
- How effective are we?





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/tcMSXNhrNrKLiP7yZzh43D>

Join at [slido.com](https://www.slido.com/join/#2286357): #2286357

(live until 5 April 2024)





Resources

- The Wolfsberg Frequently Asked Questions on Risk Assessments for Money Laundering, Sanctions and Bribery & Corruption: <https://db.wolfsberg-group.org/assets/3deb66d7-6aca-490c-bcd9-c1a3d34a807b/17.%20Wolfsberg-Risk-Assessment-FAQs-2015.pdf>Chinese Communist Party-Backed Businessman in Fiji is a Top Australian Criminal Target – OCCRP
- COSO: <https://www.coso.org/>
- COSO Internal Control Integrated Framework Executive Summary: https://www.coso.org/_files/ugd/3059fc_1df7d5dd38074006bce8fdf621a942cf.pdf
- Chinese Communist Party-Backed Businessman in Fiji is a Top Australian Criminal Target: [Chinese Communist Party-Backed Businessman in Fiji is a Top Australian Criminal Target - OCCRP](#)



Thank you.