INTERNATIONAL COMPLIANCE ASSOCIATION

Cross Border Compliance & Regulatory Tech

23 March 2023

Kigali International Financial Centre

Pekka Dare
Vice President ICA

Pekka Dare

Pekka Dare

Vice President ICA

Follow me & ICA on

https://www.linkedin.com/in/pekkadare/

https://www.linkedin.com/company/intcompassoc/mycompany/verification/

© 2020 International Compliance Association. All rights reserved.

Introduction

- Cross-border compliance refers to the set of rules, regulations, and standards that businesses must comply with when conducting their operations across different countries or jurisdictions. This includes adherence to laws related to taxation, trade, data privacy, and other regulatory requirements that apply to the company's activities in both the home country and the countries where it operates.

- Cross-border compliance is essential for multinational corporations and businesses that operate in multiple countries to ensure that they comply with local laws and regulations, maintain ethical business practices, and avoid legal and financial penalties.
- It involves understanding and adhering to the diverse and complex regulatory frameworks of various countries, as well as implementing internal controls and compliance programs that meet global standards. Effective cross-border compliance requires a comprehensive understanding of legal and regulatory requirements and a commitment to ethical business practices.

https://www.int-comp.org/insight/2022/financial-crime-within-the-metaverse/

© 2023 International Compliance Association. All rights reserved.

Regulatory Framework

- International Treaties and Agreements: The regulatory framework governing cross-border compliance is primarily established through international treaties and agreements, such as the United Nations Convention against Corruption (UNCAC) and the OECD Anti-Bribery Convention. These agreements set standards for anti-corruption measures and require countries to adopt laws and regulations to prevent and combat corruption.

- National Laws and Regulations: Each country also has its own national laws and regulations governing cross-border compliance. These laws typically include provisions related to anti-corruption, anti-money laundering, and counter-terrorism financing, and they often require companies to establish compliance programs and conduct due diligence on business partners.

- Industry-Specific Regulations: In addition to national laws and international agreements, there may be industry-specific regulations governing cross-border compliance, such as the Foreign Corrupt Practices Act (FCPA) in the United States, which prohibits US companies from bribing foreign officials to obtain or retain business.

- Enforcement Agencies: Regulatory frameworks are enforced by various agencies, such as the US Department of Justice, the UK Serious Fraud Office, and the European Anti-Fraud Office (OLAF). These agencies investigate and prosecute violations of cross-border compliance laws and regulations.

- Self-Regulatory Organizations: Some industries have established self-regulatory organizations, such as the Financial Action Task Force (FATF) in the financial sector, to promote and enforce compliance with industry-specific regulations. These organizations may set standards for compliance programs, conduct audits and assessments, and issue guidance on best practices.

© 2023 International Compliance Association. All rights reserved.

Compliance Risks

- **Bribery and Corruption**: Cross-border operations may expose companies to bribery and corruption risks, particularly when dealing with foreign officials or conducting business in countries with a high risk of corruption. Companies must ensure that they comply with anti-bribery laws and regulations, such as the FCPA and the UK Bribery Act, and implement robust anti-corruption policies and procedures.

- **Money Laundering:** Cross-border operations may also expose companies to money laundering risks, as criminals may attempt to use the international financial system to launder illicit funds. Companies must establish effective know-your-customer (KYC) and due diligence processes to identify and prevent money laundering activities.

- **Terrorism Financing**: Cross-border operations may also expose companies to the risk of terrorism financing, as terrorists may attempt to use legitimate businesses to fund their activities. Companies must comply with anti-terrorism financing laws and regulations and implement effective screening processes to identify and prevent transactions that may be linked to terrorism financing.

- **Trade Sanctions:** Cross-border operations may also be subject to trade sanctions imposed by governments, which restrict trade with certain countries or individuals. Companies must ensure that they comply with trade sanctions laws and regulations and implement effective screening processes to prevent transactions that may violate trade sanctions.

- **Data Privacy and Security:** Cross-border operations may also involve the transfer of personal data across borders, which may be subject to different data privacy laws and regulations. Companies must ensure that they comply with data privacy laws and regulations in all countries where they operate and implement robust data privacy and security measures to protect personal data

© 2023 International Compliance Association. All rights reserved.

Examples of high-profile cross-border compliance failures

- **Siemens AG**: In 2008, German engineering company Siemens AG was fined $1.6 billion by US and German authorities for violating anti-corruption laws. Siemens AG had engaged in widespread bribery to secure contracts in countries including Argentina, Bangladesh, and Venezuela. The company had also failed to implement adequate compliance controls and oversight.

- **HSBC:** In 2012, HSBC, one of the world's largest banks, was fined $1.9 billion by US authorities for facilitating money laundering and violating sanctions laws. The bank had allowed drug traffickers and other criminals to move money through its accounts and had conducted transactions with countries subject to US sanctions, including Iran and Sudan.

- **GlaxoSmithKline:** In 2014, British pharmaceutical company GlaxoSmithKline (GSK) was fined $489 million by Chinese authorities for bribery and corruption. GSK had used travel agencies to funnel bribes to doctors and hospitals in China to increase sales of its drugs. The company had also failed to implement adequate compliance controls and oversight.

- **Danske Bank:** In 2018, Danish bank Danske Bank was found to have facilitated the laundering of $230 billion in suspicious transactions through its Estonian branch between 2007 and 2015. The bank had failed to implement adequate anti-money laundering controls and had ignored warning signs of suspicious activity. The scandal led to the resignation of the bank's CEO and other top executives.

© 2023 International Compliance Association. All rights reserved.

Due Diligence

- **Mitigating Compliance Risks:** Due diligence is essential in mitigating compliance risks associated with cross-border transactions, such as bribery, money laundering, and terrorism financing. Conducting due diligence allows companies to identify and assess the risks associated with potential business partners, customers, and suppliers and implement appropriate controls to mitigate those risks.

- **Protecting Reputation:** Conducting due diligence also helps to protect a company's reputation by ensuring that it does not engage in business with individuals or entities that have a history of unethical or illegal behaviour. By avoiding association with such entities, companies can maintain a positive reputation and avoid damage to their brand.

- **Ensuring Financial Viability:** Due diligence is also important in ensuring the financial viability of potential business partners, customers, and suppliers. By conducting financial due diligence, companies can assess the financial health of these entities and avoid engaging in business with entities that may be at risk of insolvency or bankruptcy.

- **Compliance with Regulatory Requirements:** Finally, conducting due diligence is often a legal requirement in cross-border transactions, particularly in industries such as finance, healthcare, and energy. Companies that fail to conduct appropriate due diligence may be subject to legal and financial penalties, as well as reputational damage. By conducting due diligence, companies can ensure compliance with regulatory requirements and avoid costly legal and financial consequences

© 2023 International Compliance Association. All rights reserved.

Best practices for due diligence (e.g., screening potential partners, conducting site visits)

- **Conduct Screening of Potential Partners:** Companies should conduct thorough screenings of potential partners before entering into any cross-border transaction. This should include background checks on individuals, as well as assessments of their reputation and track record.

- **Visit Sites and Verify Information:** Companies should visit the sites of potential partners and verify the information provided to them. This may involve conducting on-site inspections or audits to confirm that the partner's operations are legitimate and in compliance with relevant laws and regulations.

- **Review Financial Records and Contracts:** Companies should carefully review the financial records and contracts of potential partners. This may include reviewing financial statements, tax records, and other financial data to assess the partner's financial health and risk profile.

- **Assess Legal and Regulatory Compliance:** Companies should assess the legal and regulatory compliance of potential partners, including compliance with anti-corruption, anti-money laundering, and other relevant laws and regulations. This may involve conducting a review of the partner's compliance policies and procedures, as well as assessing their compliance history and any past regulatory actions or investigations.

© 2023 International Compliance Association. All rights reserved.

Export Controls

- Export control regulations are designed to restrict the export of certain goods, technologies, and information that could be used for military or other sensitive purposes. These regulations aim to prevent the proliferation of weapons of mass destruction and other sensitive technologies.

- Export control regulations typically include licensing requirements, end-use restrictions, and destination restrictions. Companies must obtain the necessary licenses and comply with all applicable restrictions when exporting sensitive goods, technologies, or information.

- There are several international export control regimes that set common standards and guidelines for export controls. These include the Wassenaar Arrangement, the Missile Technology Control Regime, and the Nuclear Suppliers Group.

- National Export Control Laws: Many countries have their own national export control laws and regulations, which may be more restrictive than international export control regimes. Companies must comply with all applicable national export control laws and regulations in addition to international export control regimes

© 2023 International Compliance Association. All rights reserved.

Proliferation

- **Proliferation** is the transfer and export of nuclear, chemical or biological weapons; their means of delivery and related materials.
- This could include, technology, goods, software, services or expertise.

© 2022 International Compliance Association. All rights reserved.

Proliferation Financing

Proliferation finance 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*

© 2022 International Compliance Association. All rights reserved.

Proliferation Financing

- 23 October 2020 – FATF adopt amendments to recommendations 1 and 2 in respect of the risks posed by PF as detailed in recommendation 7

"financial institutions and DNFBPs should identify and assess the risks of potential breach, non-implementation or evasion of targeted financial sanctions when dealing with their customers, and take appropriate mitigating measures commensurate with the level of risks identified"

© 2022 International Compliance Association. All rights reserved.

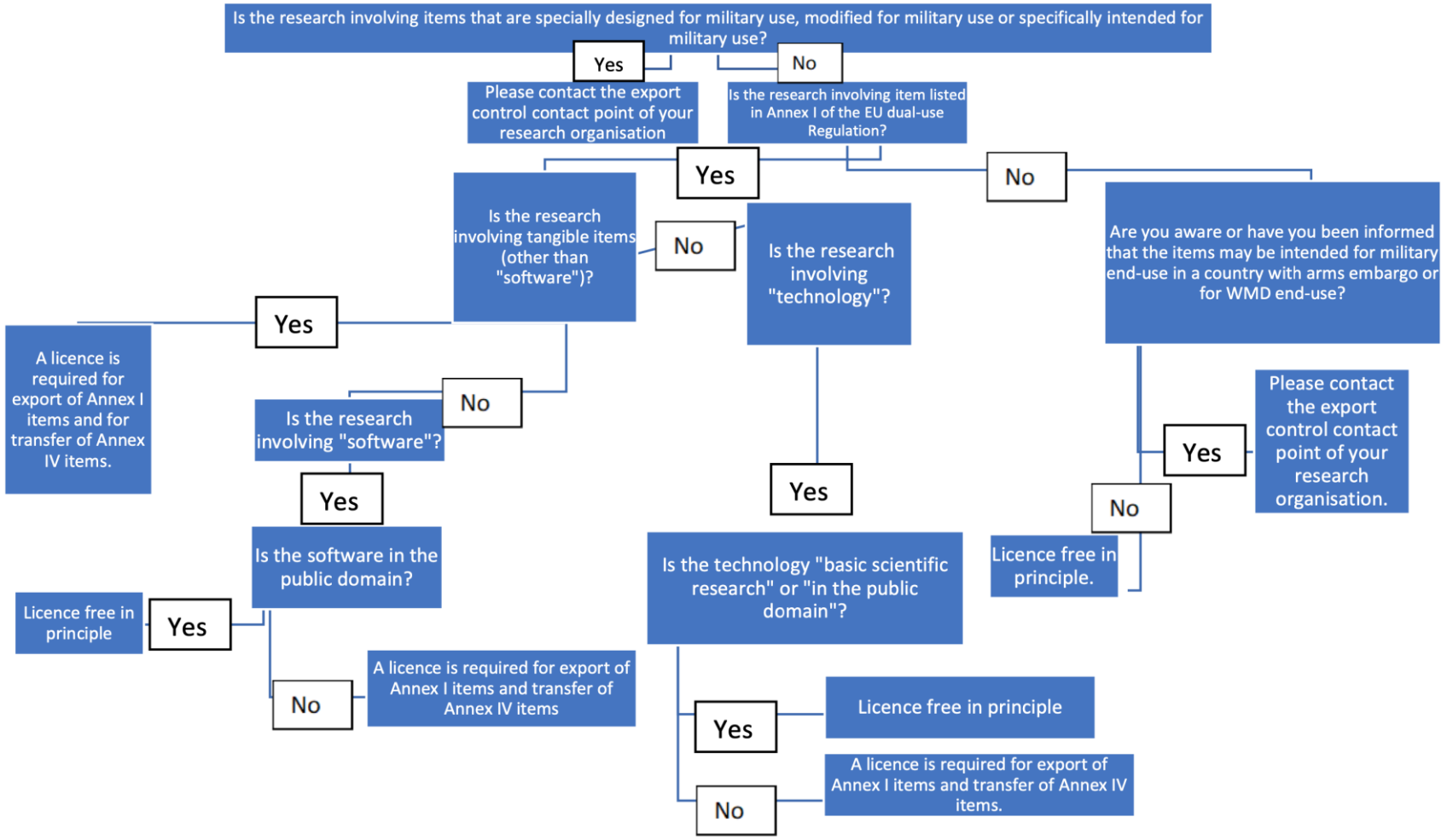
Dual-Use Goods

Category	Description
0	Nuclear materials, facilities and equipment
1	Special materials and related equipment
2	Materials processing
3	Electronics
4	Computers
5	Telecommunications and Information security
6	Sensors and Lasers
7	Navigation and Avionics
8	Maritime
9	Aerospace and Propulsion

Sub - Category	Description
A	Systems, equipment and parts
B	Test, inspection and production equipment
C	Materials
D	Software
E	Technology

© 2022 International Compliance Association. All rights reserved.

Appendix 5 - Flow chart of licence requirements for exports and intra-EU transfers of dual-use items[49]



A complex area!

[49] This scheme does not include the licence requirements for items that are specially designed or modified for military use. Please consult the relevant information provided by your competent authority. Terminology in between quotes, (i.e. “software”) refers to official definitions as provided by the EU-dual-use Regulation

https://trade.ec.europa.eu/consultations/documents/consul_183.pdf

© 2022 International Compliance Association. All rights reserved.

Complex PF Networks

PF may not necessarily be directly connected to the physical flow of goods. PF can include:

- Financial transfers
- Provision of loans
- Ship mortgages and registration fees
- Insurance and re-insurance services
- Credit lines for shipment of illicit sensitive goods
- Trust and corporate services
- Acting as an agent for, to, or on behalf of someone else
- Facilitation of any of the above.

In many cases PF activity has the sole aim of generating access to foreign currency and the international financial system. It may look like a legitimate trading transaction.

© 2022 International Compliance Association. All rights reserved.

FIs/DNFSB and PF Exposure

- **Front companies**, i.e. companies that appear to undertake legitimate business but which, in reality, serve to obscure illicit financial activity
- **Shell companies**, i.e. inactive companies used as a conduit for money that do not have a high level of capitalisation or which displays other shell company indicators such as long periods of account dormancy followed by a surge of activity
- **Brokers and professional intermediaries** to obtain trade finance products and services, or as parties to clean payments.
- **Nationals or dual citizens** of States that undertake Proliferation, or **family members** of such persons, used as intermediaries in countries not of Proliferation concern, to facilitate procurement of goods and/or for payment of funds. Likely to involve use of personal banking products.

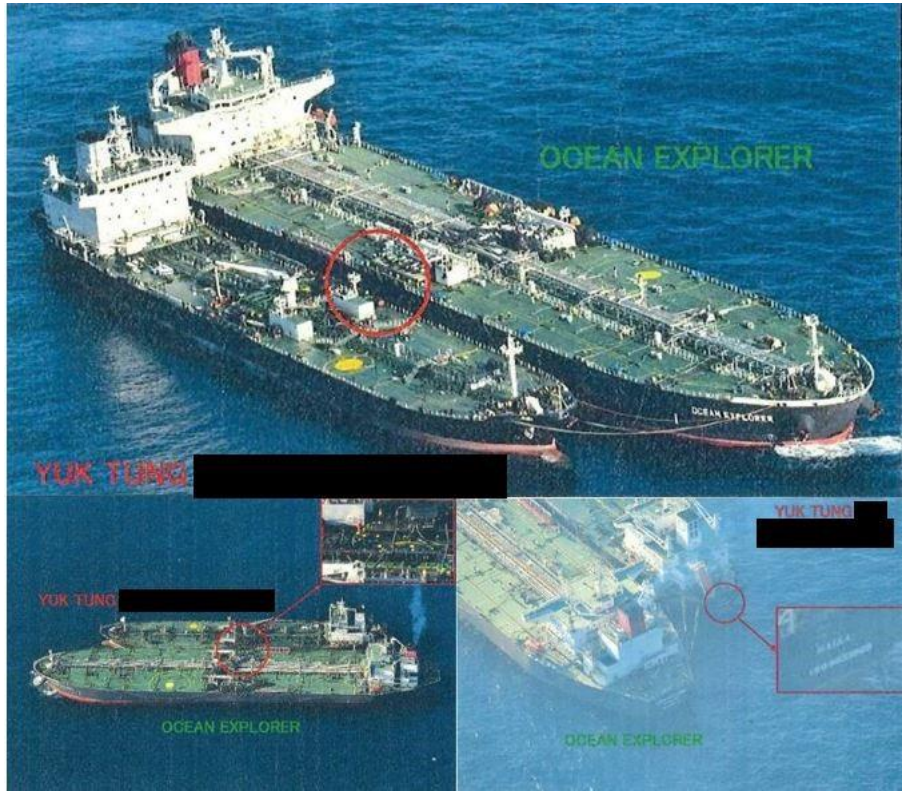
© 2022 International Compliance Association. All rights reserved.

Messages for Firms

- Private Sector should identify and assess PF risks – develop policies and controls under existing frameworks. PF relates to Sanctions being evaded or not implemented.
- Proliferation networks becoming smarter- according to UN expert reports. Evasion using opaque entities and complex structures
- FATF relies on Risk Based Approach: Complex structures = High Risk = EDD

© 2022 International Compliance Association. All rights reserved.

North Korea: Holes in the Sanctions Wall



© 2020 International Compliance Association. All rights reserved.

UN Report on North Korea

- Illegal ship to ship transfers Oil, petroleum coal etc
- Cyber attacks and focus on financial firms
- Cryptocurrency exchanges attacked
- Use of Diplomats
- Front Companies & trade
- Bulk Cash smuggling
- Insurance Firms and Banks a focus

© 2020 International Compliance Association. All rights reserved.

Illicit generation of revenue through cyberactivities

- DPRK continuing to target financial institutions and cryptocurrency firms and exchanges.
- DPRK stole more than $50 million between 2020 and mid-2021 from at least 3 crypto exchanges in North America, Europe and Asia.
- DPRK a stole a total of $400 million of crypto in 2021 through seven intrusions into crypto exchanges and investment firms.
- Cyberattacks used phishing lures, code exploits, malware, and advanced social engineering to siphon funds out of these organizations' Internet-connected 'hot' wallets into DPRK controlled addresses.
- The crypto funds acquired by the DPRK go through a careful money-laundering process in to be cashed out.

Figure IV
New intercontinental ballistic missile[22] at "Self-Defence 2021" exhibition

Source: Korean Central Television, 12 October 2021.

© 2020 International Compliance Association. All rights reserved.

Banks & Evasion: Common Themes?

Sudan, Iran, Cuba

- Cover Payments
- Use of Special Purpose Vehicles
- Poor Systems and Controls
- US Clearing
- Culture/Senior Management
- Lack of transparency with Regulators

OFAC
Office of Foreign Assets Control

https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20140630_bnp_settlement.pdf
https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/121210_SCB_Settlement.pdf
https://www.treasury.gov/resource-center/sanctions/CivPen/Documents/20150312_commerzbank_settlement.pdf

© 2020 International Compliance Association. All rights reserved.

Iran Sanctions Evasion Network

- The scheme, between 2013 and 2017, involved Panama-based front company East & West Shipping purchasing two liquid petroleum tankers to ship Iranian oil.
- Ownership of the vessels was then transferred to other entities, and controlled by another Mokhtari-linked firm, Greenline Shipholding.
- FBI investigators uncovered emails showing Greenline deployed the two vessels "to transport Iranian petrochemical products from Iranian ports to other locations and to participate in ship-to-ship transfers of Iranian products while on the high seas".
- The network used false shipping documents to hide any link to Iranian goods
- As part of his guilty plea, Mokhtari must forfeit US$2.86m as well as assets derived from illicit Iranian oil trading, & a US$1.5mn property in California.
- In November, authorities took action against a network of **fuel traders** accused of facilitating the sale of Iranian-origin oil.
- That action followed Treasury sanctions against six companies facilitating the sale of Iranian oil to buyers in East Asia

https://www.gtreview.com/news/global/iran-sanctions-evasion-network-used-uae-panama-front-companies/

© 2020 International Compliance Association. All rights reserved.

Iran’s secret network of front companies

- The oil itself is fairly easy to deliver under the radar by using ship-to-ship transfers in open water and then blending it in foreign ports with other crude to disguise its origin. The greater difficulty for Iran is getting paid for the sales without triggering red flags in the international financial system. Instead of selling the oil directly to the end buyer, it is sold via front companies, often to other front companies.

“The individuals running this illicit network use a web of shell companies and fraudulent tactics including document falsification to obfuscate the origins of Iranian oil, sell it on the international market, and evade sanctions,”

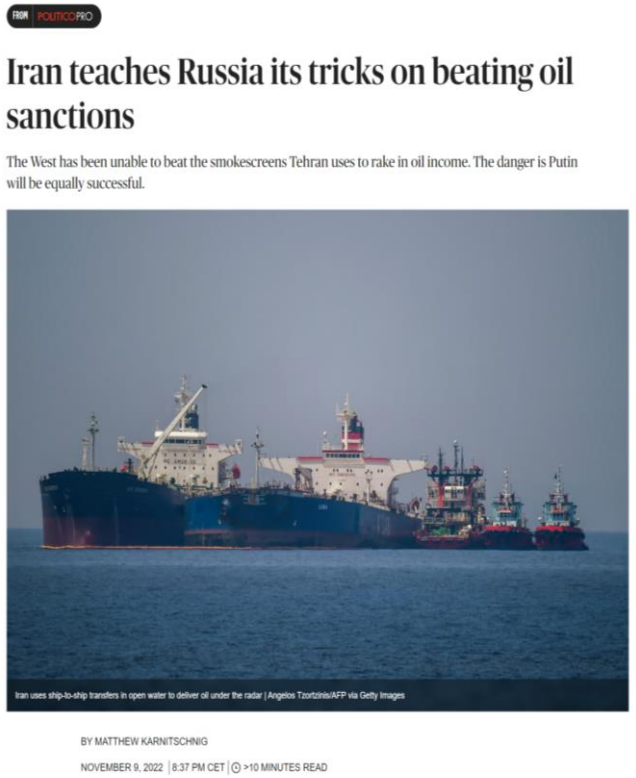
- Iran’s surreptitious financial system is built on what are known in the country as “money exchange houses.” The organizations, which number in the dozens, are Iran-based clearinghouses that operate a network of front companies abroad,
- If an Iranian firm needs to undertake a foreign transaction prohibited by sanctions, its local bank can turn to one of the houses to filter the payment through a labyrinth of front companies, making it extremely difficult to trace the true origin, Western diplomats say.

https://www.politico.eu/article/iran-russia-cooperation-dodging-oil-sanctions/

© 2020 International Compliance Association. All rights reserved.

Iran’s Sanction Evasion Methods

- Iran uses a network of front companies and foreign banks — incl major institutions in Europe & the U.S. to evade international controls and conduct business abroad.
- A cache of recent transaction data reviewed by POLITICO between Iranian clearing houses and foreign-registered front companies controlled by the regime suggests that the volume of sanctions-evading transactions handled by the network is at least in the tens of billions of dollars annually.
- While Iran’s oil exports have roughly halved under the sanctions to about 1 million barrels per day, it has succeeded in maintaining robust trade in other areas, such as petrochemicals and metals. At about $100 billion last year, Iran’s foreign trade reached its highest level since the U.S. reimposed sanctions. Despite the drop in oil volumes, the country has recently benefited from rising prices, with export revenue last year more than doubling to about $19 billion. What’s driving Iran’s oil recovery, according to the World Bank, are “indirect exports to China.”
- Iranian oil is attractive to China, mainly because it’s relatively cheap. The illicit nature of sanctioned Iranian crude means it sells at a steep discount to market prices.



FROM POLITICO PRO

Iran teaches Russia its tricks on beating oil sanctions

The West has been unable to beat the smokescreens Tehran uses to rake in oil income. The danger is Putin will be equally successful.

Iran uses ship-to-ship transfers in open water to deliver oil under the radar | Angelos Tzortzinis/AFP via Getty Images

BY MATTHEW KARNITSCHNIG

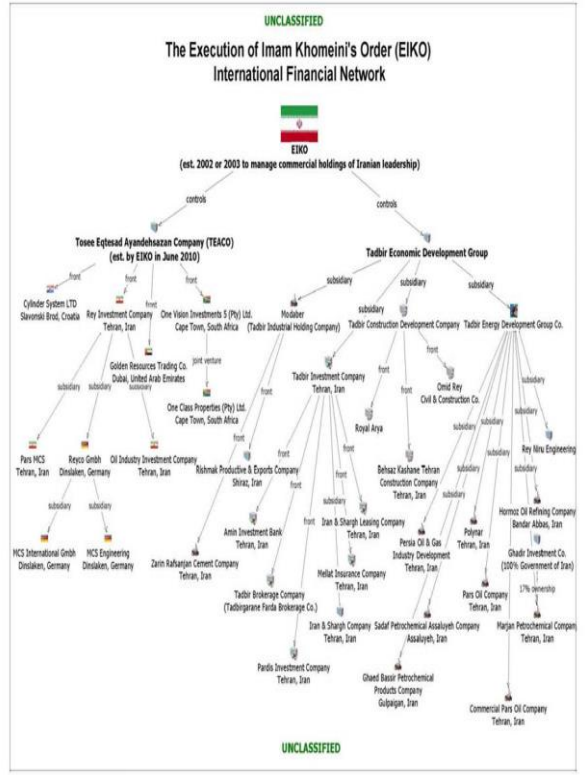
NOVEMBER 9, 2022 | 8:37 PM CET | >10 MINUTES READ

https://www.politico.eu/article/iran-russia-cooperation-dodging-oil-sanctions/

© 2020 International Compliance Association. All rights reserved.

Link to Western Banks

- Many of the transactions, which involve everything from oil to scrap metal, are in euros or dollars which requires the involvement of a European or U.S. bank. ‘
- Major EU & U.S. banks have been used by Iran to settle these transactions. Under U.S. sanctions rules, domestic banks and foreign banks that do business in the U.S. are prohibited from conducting almost all financial dealings that involve Iran.
- No evidence the banks were aware the transactions were part of Tehran's schemes. If the front companies named in the transactions haven't been specifically designated by the U.S. government, the banks often fail to detect the suspect activity.
- One of the companies that appears frequently in the transactions is Hong Kong-registered Hua Gong HK Trading Ltd. It was founded in October of 2018, shortly after the U.S. began to reintroduce sanctions against Iran. Western diplomats say the firm is a front company operated by Tahayyori Guarantee Society, one of Iran’s biggest exchange houses.
- Hua Gong transactions over the past year reviewed by POLITICO passed through both Deutsche Bank and Citibank via Chinese banks. The recipients of the funds it transferred included firms in Hong Kong, Italy and Singapore.



Source: U.S. Treasury Dept.

https://www.politico.eu/article/iran-russia-cooperation-dodging-oil-sanctions/

© 2020 International Compliance Association. All rights reserved.

Considerations for Firms

- Name Screening is not enough! Need to identify if North Korea or Iran are behind entries you are dealing with

- UK First PF National Risk Assessment in Sep 21- UK Financial Sector at highest risk.
- Iran and DPRK have been subject for sanctions for a long time so very astute and used to scrutiny – don't do business in their own names. **Name list screening alone is not going to help you.**
- Networks are complex, use shell companies, intermediaries and secrecy jurisdictions.

© 2022 International Compliance Association. All rights reserved.

Integrating Red Flags

- Inputs can be benign e.g. Dual Use Goods often don’t raise eyebrows (context is key!) FI often not party to underlying transactions so could be hiding in plain sight (vast number of listed Dual Use Goods makes it challenging eg scuba gear, video game consoles). FIs wont see the whole intelligence picture.
- Often a red flag involvement if a strange third party in a transaction between a buyer and a seller?
- UK National Risk Assess identifies Front and shell Companies and complex structures with use of intermediaries.
- Also red flags include falsification of documents to get insurance for a sanctioned Iranian entity
- Be aware of the Risk Factors published by the FATF Working Groups

© 2022 International Compliance Association. All rights reserved.

Changing Risks

- An increase in complex ownership structures being used in PF networks
- FATF also published new indicators in maritime and Trade Finance Transactions.
- If you identify only a single indicator may not be definitely a sanctions issue but requires enhanced scrutiny and or monitoring
- Often STRs from firms don’t initially identify PF more often ML
- Rare to have STRs initially definitely related to PF. Will often lead to blocking and Reporting by FIs/ DNFSB.
- Many firms using a smaller list of PF sensitive goods to focus on (smaller set than the 1000’s of Dual Use Goods) and to clearly link these to typologies.

© 2022 International Compliance Association. All rights reserved.

Undertaking a PF Risk Assessment

- RBA- must assess PF risk for your firm, mitigate and allocate resources to highest risk areas.

- FATF – gives guidance on how to undertake a PF Risk assessment Guidance on new sectors step by step including trade finance, Correspondent banking and VASPs
- New indicators available based on UN Expert Panel reports and typologies. **KNOW YOUR ENEMY!**
- DPRK using traditional and new methods Crypto Exchange attacks / Spear Phishing and traditional movement of funds through engaging with Banks overseas.
- Iran also using 3rd parties/ collaborators and 3rd countries

© 2022 International Compliance Association. All rights reserved.

PF Risk Assessment for Firms

- Risk assessment is iterative
- Key is for FIs & to have a wider Financial Crime Risk assessment programme **not just Money Laundering** (include economic sanctions) .
- Firms must understand sanctions evasion techniques and not just treat sanctions as a list screening exercise! Because targets are not acting out of Iran and DPRK and not using their real names.
- FIs need a dedicated resource and written methodology for doing a fin crime risk assessment that includes PF.
- MUST include 1st Line of Defence as they own the data.
- Follow through from Enterprise Wide Risk Assessment (EWRA) to individual Risk Assessment Methodology.
- Must also have an overall Board level C-suite clarity of risk appetite firm wide clarity e.g. on appetite for dealing with higher risk jurisdictions and industries.
- Use other tools to manage risk , such as enhanced monitoring, ring fencing, warranties and exit.

© 2022 International Compliance Association. All rights reserved.

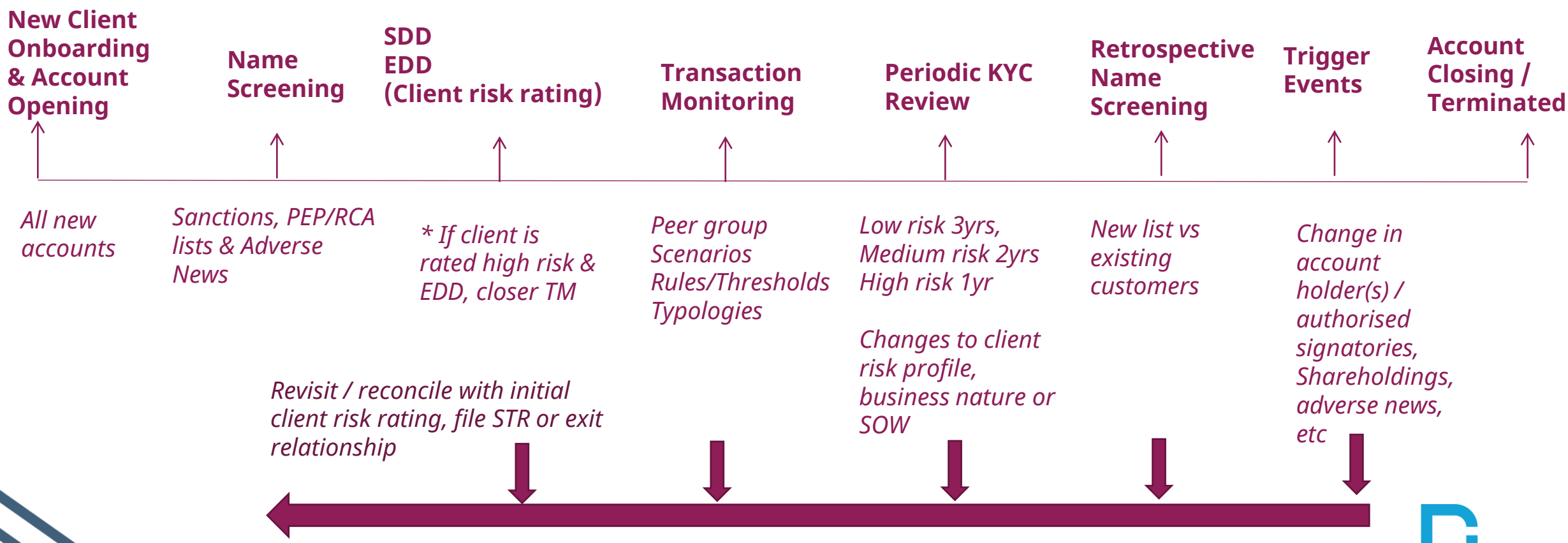
Sanctions Screening

A firm should have effective, up-to-date screening systems appropriate to the nature, size and risk of its business

- Do you know which screening solutions are used in your firm at a high level?
- Who is responsible for maintaining these?
- What factors will be taken into consideration when choosing solutions?
- How are screening tools maintained?
- What does fuzzy logic mean?

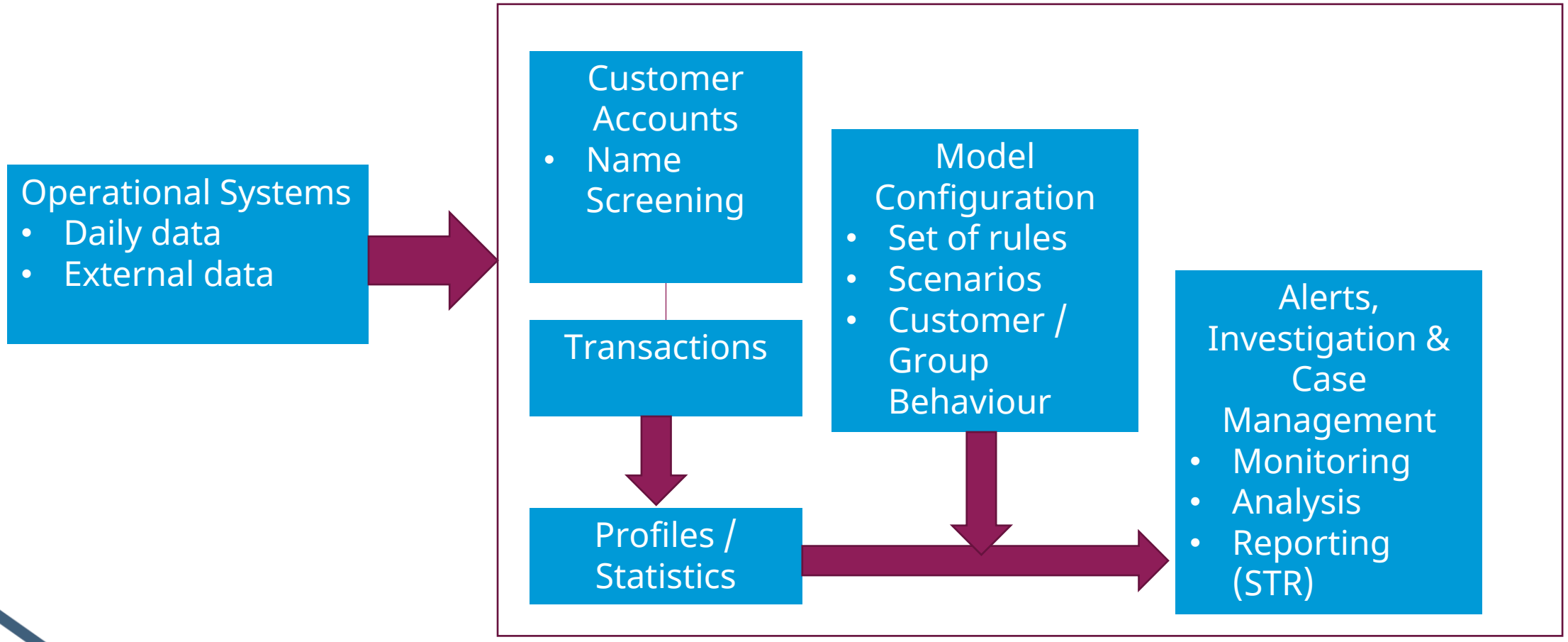
© 2022 International Compliance Association. All rights reserved.

Overview of KYC and Screening Process



© 2022 International Compliance Association. All rights reserved.

Legacy TM System Architecture Overview



Source: FICO Tonbeller

© 2022 International Compliance Association. All rights reserved.

How Systems Work…Fuzzy Logic Name Screening – what and why?

- **Fuzzy Logic name screening & matching –** Set of algorithms, rules, synonym tables, foreign word transliterations, and other functionalities designed by the vendor to generate name matches between client data and watchlist content.
- The fuzziness of the logic creates space for the matching of **inexact, but likely similar**, names / data. For e.g.:
  - **Probabilistic logic, phonetics matching** - Matches words that are similar when said aloud to augment direct matching.
  - **Deterministic logic** - Allowing for a thorough evaluation of the performance of the watchlist screening model's match scoring algorithm and thresholds.

© 2022 International Compliance Association. All rights reserved.

How TM Systems Work(ed)…Rules and Scenarios

- **Rules** - three categories: i) volume or frequency, ii) structuring, or iii) velocity. Rules identify anomalies - e.g.: abnormally high volume of transactions or patterns of transactions falling within an institution's internal threshold ("if, then" logic).
- **Customer / Group behaviour-based logic** - Relies on the customer's historical or expected behaviors. This logic looks for deviations from accepted peer group norms or from the customer's historical patterns.
- **Scenarios** - Based on known ML/TF typologies. E.g., Multiple deposits into same account and quick withdrawal.

© 2022 International Compliance Association. All rights reserved.

Who/what should be screened?

© 2020 International Compliance Association. All rights reserved.

Who should be screened?

Customers	Individual and legal entity customers
Staff	All staff
Third Party Service Providers	All third party service providers. Including suppliers (such as suppliers of screening solutions, or staffing); those renting properties from the firm etc.
Connected/Related Parties	Identified to be connected to the business relationship or Sanctioned target
UBOs	Ultimate Beneficial Owners (and key parties to the business relationship)
Products & Services	Eg Transactions

© 2020 International Compliance Association. All rights reserved.

What should be screened?

Countries/jurisdictions	Against prohibited countries
Sensitive words	E.g. in transaction reference fields
Customer products	E.g. for potential dual use goods

© 2020 International Compliance Association. All rights reserved.

Customer Alert Investigations

- When a customer's name matches a person on the an external/internal watchlist; an alert is generated
- Alerts may be generated where the names are similar (but not exact) which warrants further investigation – these are known as potential matches
- Firms are required to have procedures in place to investigate potential matches to identify whether they are
  - False matches? ; or
  - True matches
- Using a risk based approach
- Firms are required to have procedures in place for actions to be taken in the event a true match is confirmed

© 2020 International Compliance Association. All rights reserved.

Payment Alert Investigations

The first step is to understand the information contained in within the message fields of the payment types, for example MT202 swift message (cover payment) below:

Status	Tag	Field Name
M	20	Transaction reference number
M	21	Related reference
M	32A	Value date, payment code, inter-bank settled amount
O	52A	Ordering Institution
O	53A	Sender's correspondent
O	56A	Intermediary bank institution
O	57A	Account with institution
M	58A	Beneficiary institution
O	72	Bank to bank Information

© 2020 International Compliance Association. All rights reserved.

Payment Alert Investigations

Status	Tag	Field Name
M	20	Transaction reference number
M	23B	Bank operation code
O	23E	Instruction Code
M	32A	Value date, payment code, inter-bank settled amount
O	33B	Debit account currency/ instructed amount
M	50K	Ordering Customer
O	52A	Ordering Institution
O	56A	Intermediary bank institution
O	57A	Account with institution
M	59A	Beneficiary customer
O	70	Remittance information
M	71A	Details of charges
O	72	Bank to bank information

© 2020 International Compliance Association. All rights reserved.

Case Study

What do the message fields in this payment message tell you?

Senders Reference

ABC3456789

Currency/Amount

USD 2,100

Date

28/07/2014

50: Ordering Customer

Filmtech
London
UK

52: Ordering Institution

Bank A, UK

53: Senders Respondent

56: Intermediary Bank

57: Account with

Bank B, Singapore

58/9: Benef.Inst/Cust

Logifilm

72: Sender to Receiver

70: Payment Details

Payment to supplier Aazam

© 2020 International Compliance Association. All rights reserved.

Case Study

What do the message fields in this payment message tell you?

Senders Reference

QRS987654T

Currency/Amount

Euro 70,000

Date

09/01/2015

50: Ordering Customer

Trade Co.
Zurich

52: Ordering Institution

Bank C, CH

53: Senders Respondent

56: Intermediary Bank

57: Account with

Bank D,

58/9: Benef.Inst/Cust

School International De Geneve
1208 Geneva

72: Sender to Receiver

70: Payment Details

Textbook Natural Sciences

© 2020 International Compliance Association. All rights reserved.

The Cost of Getting it Wrong

© 2020 International Compliance Association. All rights reserved.

Bribery & Corruption ‘Extraterritoriality’




TRANSPARENCY INTERNATIONAL
the global coalition against corruption

Search

About | What we do | Countries | Campaigns | Donate | News | Blog | Press | Library

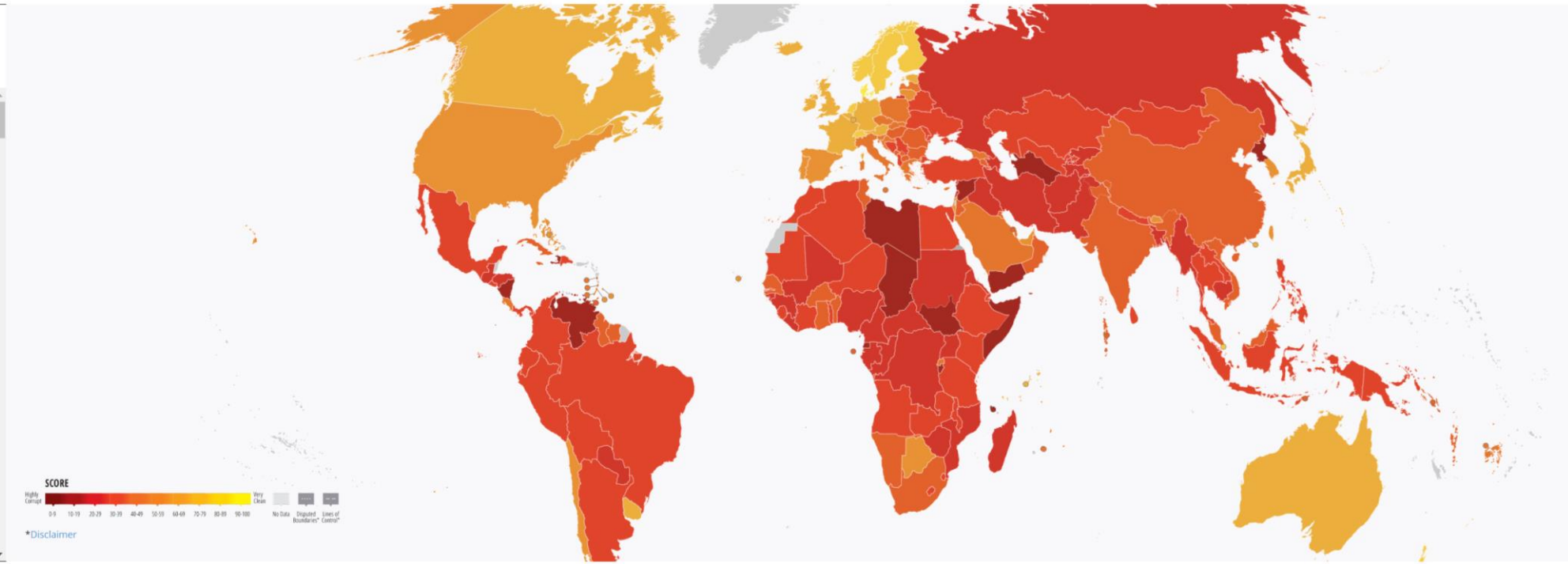
Home / CPI

CORRUPTION PERCEPTIONS INDEX

2022

Search

Score	Country	Rank
90	Denmark	1
87	Finland	2
87	New Zealand	2
84	Norway	4
83	Singapore	5
83	Sweden	5
82	Switzerland	7
80	Netherlands	8
79	Germany	9
77	Ireland	10
77	Luxembourg	10
76	Hong Kong	12
75	Australia	13
74	Canada	14
74	Estonia	14



*Disclaimer

An Issue In “Developed” Economies

thejournal.ie Contribute : Support us now

Irish News FactCheck Voices Brexit Covid-19

Sixth person arrested over alleged corrupt practices at Kildare and Wicklow Education Training Board

The man in his 30s was arrested this morning.

Dec 7th 2020, 2:48 PM 17,996 Views 0 Comments Share 8 Tweet Email 1

A SIXTH PERSON has been arrested by gardaí as part of an ongoing investigation into alleged corrupt practices at the Kildare and Wicklow Education Training Board (KWETB).

Gardaí attached to the Garda National Economic Crime Bureau (GNECB) arrested a man in his 30s this morning.

The operation was conducted as part of Operation Lakefront by detectives attached to the Anti-Corruption Unit, the GNECB, in Co

THE TIMES THE SUNDAY TIMES netwealth
Wednesday, March 24, 12:00-1:00PM (GMT)
REGISTER HERE

Prison looms after police intercepted ‘burner’ phones to bring down Nicolas Sarkozy

Nicolas Sarkozy with his wife, Carla Bruni-Sarkozy. She posted on Instagram next to an image of the couple embracing and with the hashtag #Injustice
THE MEGA AGENCY

Nicolas Sarkozy, the president of France from 2007 to 2012, was sentenced to a year in prison yesterday on charges of offering a bribe to a judge in return for information.

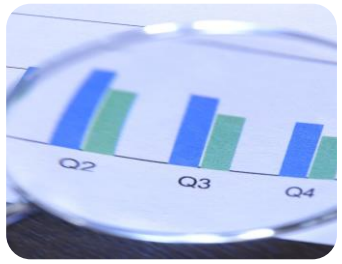
Sarkozy, 66, announced an appeal, a step that keeps him out of jail until another full trial has been completed. The former centre-right president is the first modern French leader to be convicted of corruption. He was sentenced with Thierry Herzog, his lawyer, and Judge Gilbert Azibert to one year of imprisonment and two suspended. Herzog was also barred from practice for five years.

Anti Bribery & Corruptions: 6 Pillars

Proportionate Procedures

Senior Management Buy In

Risk Assessment



Due Diligence

Training & Communication

Monitoring

Bribery Red Flags

- Unusual Payment Patterns or Financial Arrangements.
- A History of Corruption in the Geography or Industry.
- Unusually High Commissions.
- Lack of Transparency in Expenses and Accounting Records.
- Apparent Lack of Qualifications or Resources.
- Recommendation by a Government Official
- Negative News Media

Bribery & Corruption: Best Practice in Managing Risk

3 Key Risk Areas + Controls

Hiring Policies	+ Connected Hire Policies
Associated Persons	+ AP registers/ Due Diligence
Gifts and Hospitality	+ Proportionate Policies

Across ALL : Risk Assessment and Monitoring

Data Privacy

- International data transfers are governed by a variety of data privacy regulations, such as the EU General Data Protection Regulation (GDPR), the UK Data Protection Act 2018 and the California Consumer Privacy Act (CCPA), which impose certain restrictions on the cross-border transfer of personal data.

- One of the key requirements for cross-border data transfers is that the data must be protected by adequate safeguards, such as standard contractual clauses or binding corporate rules, to ensure that the data remains protected even when it is transferred outside of its country of origin.

- In addition to the requirement for adequate safeguards, data privacy regulations often require that organizations obtain explicit consent from individuals before transferring their personal data across borders. This consent must be informed and freely given, and individuals must be given the right to withdraw their consent at any time.

- Failure to comply with data privacy regulations governing cross-border data transfers can result in significant legal and financial consequences for organizations, including fines and reputational damage. As such, it is important for organizations to understand the requirements of the relevant regulations and to implement appropriate measures to ensure compliance.

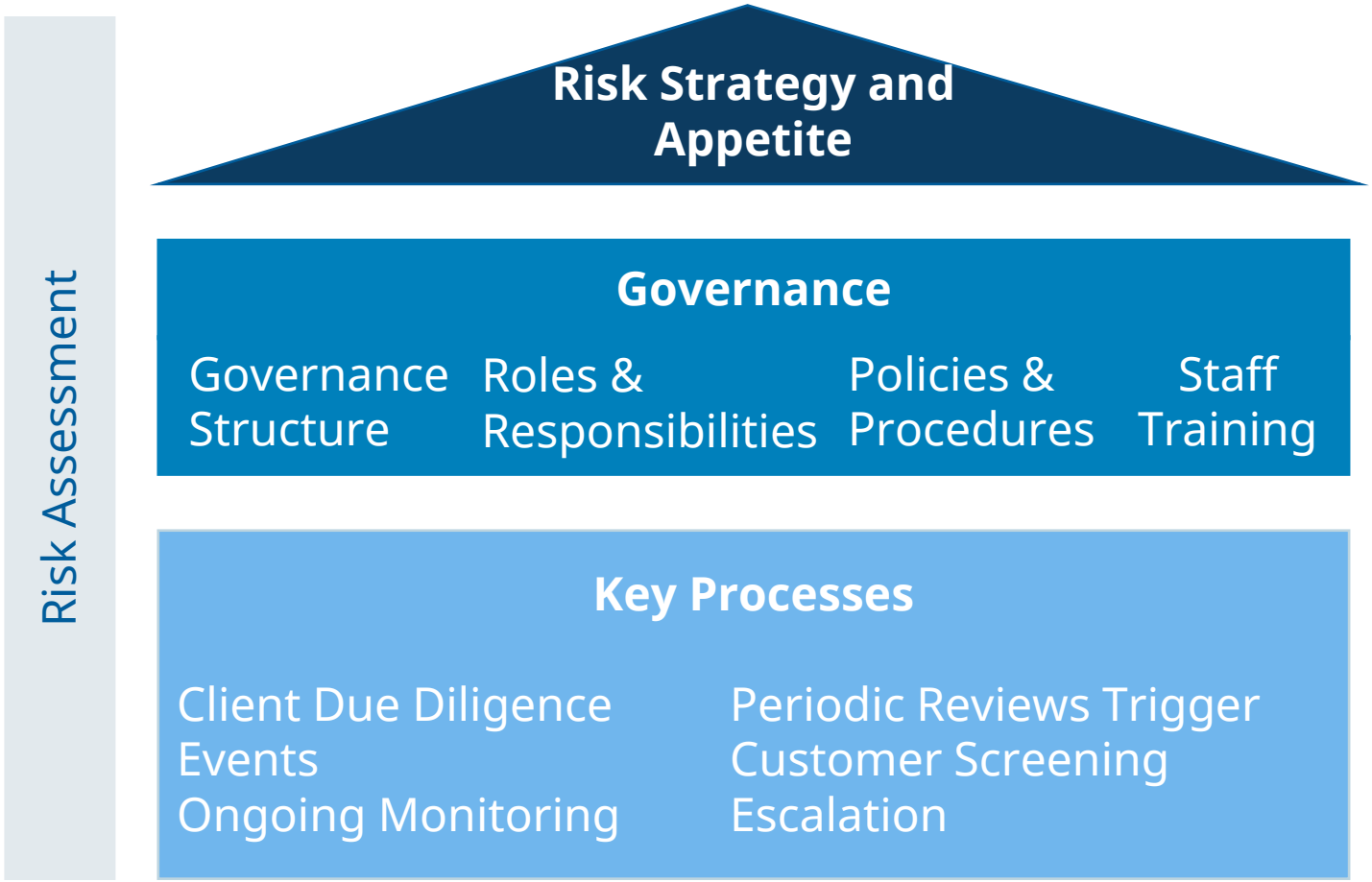
© 2023 International Compliance Association. All rights reserved.

Compliance Programs

- Importance of establishing a comprehensive compliance program for cross-border operations
- Elements of an effective compliance program (e.g., policies and procedures, training, monitoring)

© 2023 International Compliance Association. All rights reserved.

Organising Financial Crime Controls

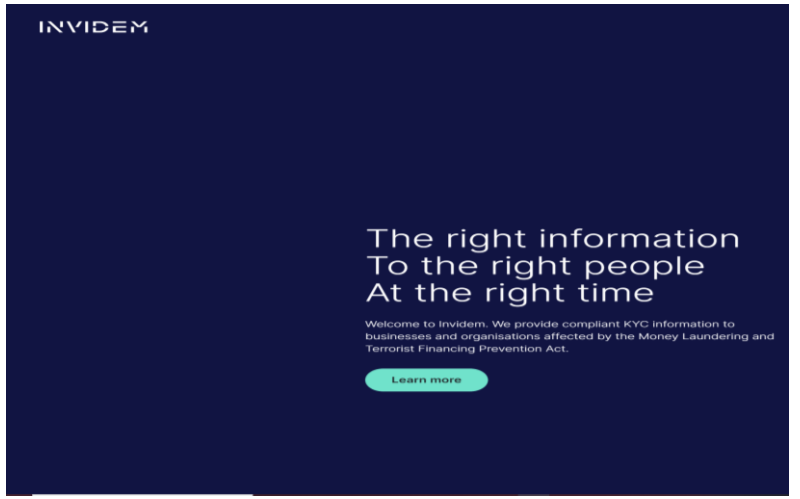


Regulatory Tech

© 2020 International Compliance Association. All rights reserved.

Global Trends

- Increased cooperation b/w Public & Private Sector
  - COSMIC –Singapore MAS & 6 Major Banks
  - JMLIT UK 2015- FATF endorses 20+countries with similar partnerships
  - KYC Manual to more Tech shared solutions (SaaS) KYC Utilities finally take off?
  - Cooperation between Banks (See TMNL) TM Netherlands

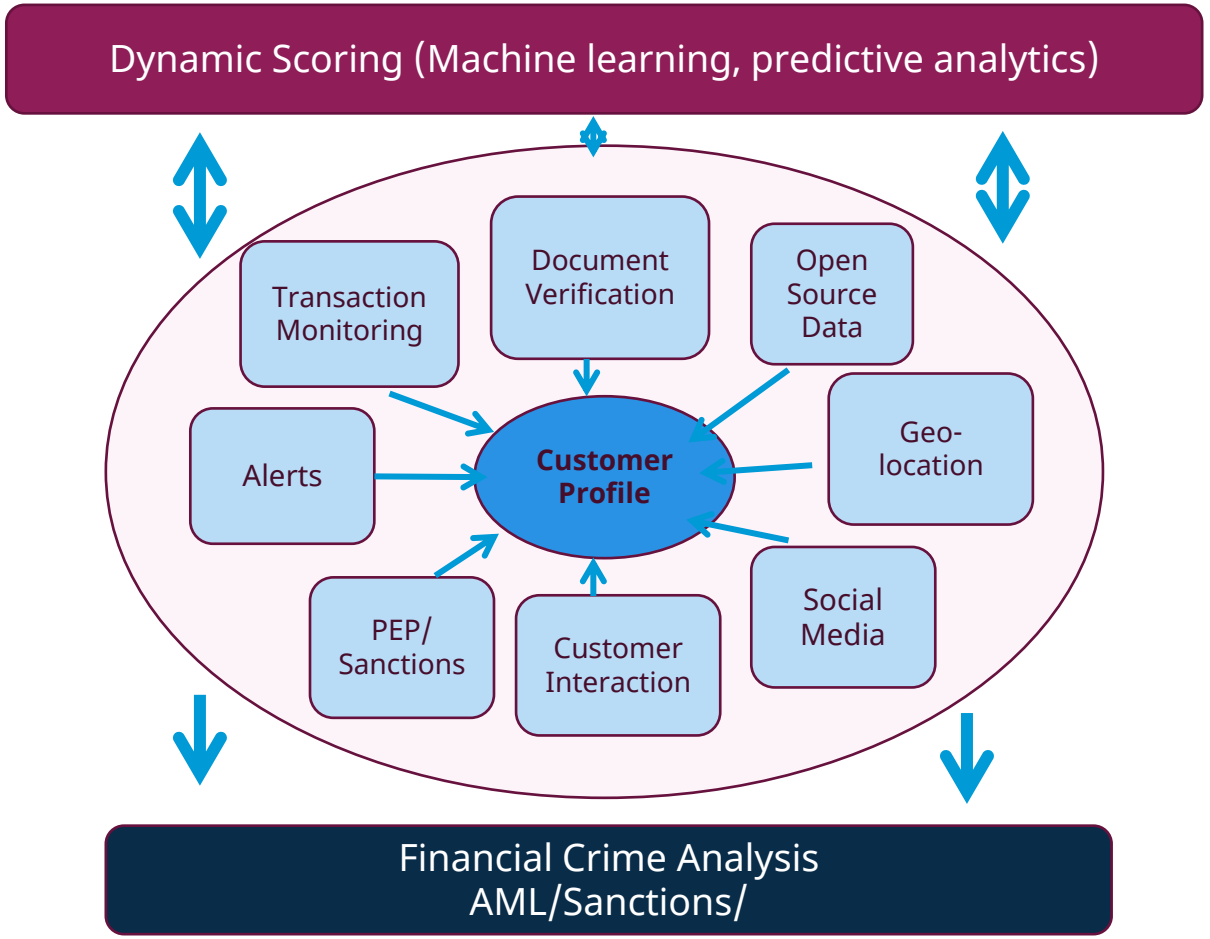


https://www.mas.gov.sg/news/media-releases/2021/mas-and-financial-industry-to-use-new-digital-platform-to-fight-money-laundering

© 2020 International Compliance Association. All rights reserved.

New Age TM System Architecture Overview…

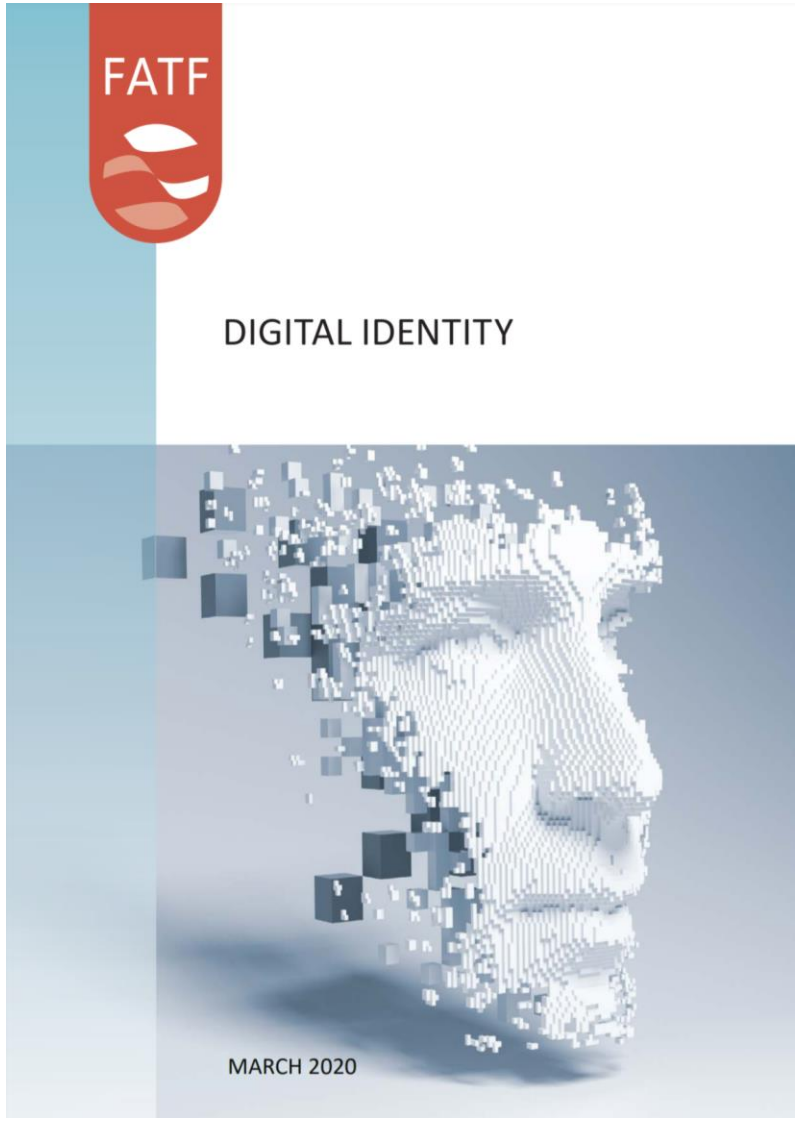
- New Age TM System - More expensive? (Consider time saving)
- Technology is used to:
  1) Reduce false positives
  2) Identify greater range of alerts
- Network Linkage Analysis, or Social Graph Analysis
- Takes critical data elements
- Builds up a network of connected entities
- Finds commonalities
- Might provide a reason for further analysis
- Helps draw conclusions not found from a single piece of information



© 2020 International Compliance Association. All rights reserved.

Global Trends

- Reg Tech & AI benefits continue for Firms
- Banks/ Fin Tech and Regulators a dynamic relationship
- Emerging and smaller markets slower to accelerate digitisation
- Understanding risk vs Black Box IP
- Digital First- Digital Banks, Digital ID & V growing fast.



© 2020 International Compliance Association. All rights reserved.

Vendor Presentation

Product Video - Ident & eSign

Identification and conclusion of contracts in less than 4 minutes

1. The prospective customer chooses a product on the website.

   Start of the TrueID process.

2. ID specialist identifies prospects through the TrueID software.

   Optional: Signing of a contract with a qualified electronic signature as part of a video chat.

3. Immediate transmission of identification and contract data to the partner.

   The prospect becomes a client and can instantly use the product.

© 2020 International Compliance Association. All rights reserved.

Vendor Presentation

Product AutoIdent

AutoIdent is the fastest way to verify your customer's identity

1. Verifies customer's ID document in real-time.

   Easy to follow on-screen prompts for best-in-class conversion rates.

2. Secure face recognition made easy through a familiar selfie style tool.

3. Automated extraction of data.

   Verification of ID authenticity.

   Results available in real-time.

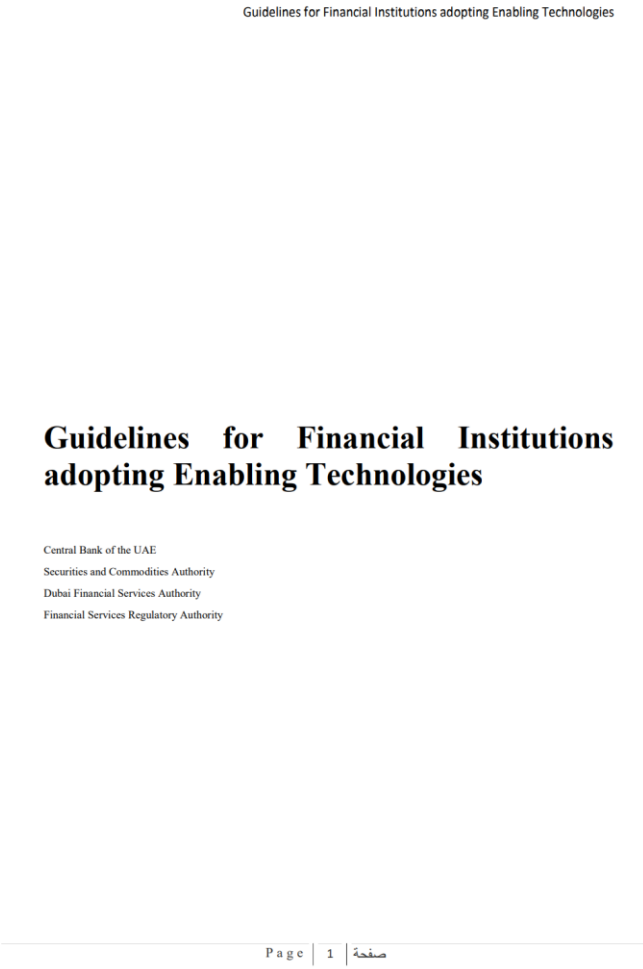
Take a picture of the front of your ID

Take a selfie

Complete. You are done. Please select the button to finish the identification process.

© 2020 International Compliance Association. All rights reserved.

Regulatory Approaches: Group Review



https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf

https://www.fca.org.uk/publication/research/research-note-on-machine-learning-in-uk-financial-services.pdf

https://365343652932-web-server-storage.s3.eu-west-2.amazonaws.com/files/2316/3687/7526/Guidelines_for_Financial_Institutions_adopting_Enabling_Technologies_20211107.pdf

© 2020 International Compliance Association. All rights reserved.

Key Consideration in evaluating a Reg Tech Vendor

- Interoperability
- Ongoing Support
- A partnership approach?
- Material Outsourcing Requirements
- Reputation
- Testing & flexibility
- QA & external validation eg ISO or recognised standards body
- Ability to provide explainibility tools
- Approaching regulator

© 2020 International Compliance Association. All rights reserved.

Extract from the Financial Action Task Force (FATF) Guidance on Digital Identity

SECTION V: ASSESSING WHETHER DIGITAL ID SYSTEMS ARE SUFFICIENTLY RELIABLE AND INDEPENDENT UNDER A RISK-BASED APPROACH TO CDD

Question One: Is the digital ID system authorised by government for use in CDD?

142. Under Question One, where the government "stands behind" a digital ID system and has deemed it appropriate for use in CDD, regulated entities can use the digital ID system without performing the assessments under Question Two and Three. The government has in effect conducted both steps of the recommended assessment—at least for standard CDD risks—for the regulated entities and the remaining parts of the decision process do not apply. However, depending on AML/CFT laws and the digital ID ecosystem in the jurisdiction, regulated entities may be required to take additional measures (see paragraphs 147 and 148 below).

143. Governments may explicitly deem a digital ID system to be appropriate for use in CDD by issuing regulations or providing guidance to regulated entities, either permitting or requiring regulated entities to use the digital ID system(s) for certain aspects of CDD. Explicit authorisation may occur, for example, when the government developed and operates the digital ID system(s) and therefor has confidence in them, or when the government has a mechanism for obtaining audited, certified information on the assurance levels of another provider's digital ID system.

© 2020 International Compliance Association. All rights reserved.

Extract from the Financial Action Task Force (FATF) Guidance on Digital Identity

144. Governments may also implicitly "stand behind" and deem a digital ID system appropriate for regulated entities to use in CDD. That could be the case, for example, when the government provides a general-purpose digital ID system that is used to prove official identity, whenever required in the jurisdiction. Governments should be transparent about how its digital ID system works and its relevant assurance levels. The same is true for its limited-purpose identity systems, authorised for use in the financial sector.

145. Depending on domestic AML/CFT laws and regulations, regulated entities will need to supplement the use of authorised digital ID systems in certain circumstances, including for example, higher risk situations and to collect information on other aspects of CDD not covered for the purposes of this Guidance (i.e. understanding the purpose and intended nature of the business relationship). Some jurisdictions may have regulations only authorising the use of digital ID systems only for lower risk situations.

146. Apart from their jurisdiction's regulatory requirements, regulated entities are encouraged to consider whether they should adopt additional digital ID risk mitigation measures (if available), such as additional identity attribute data points or additional authenticators, and/or ML/TF risk mitigation measures, given the financial institution's own AML/CFT, anti-fraud, and general risk management policies.

© 2020 International Compliance Association. All rights reserved.

Extract from the Financial Action Task Force (FATF) Guidance on Digital Identity

Question Two: Do you know the relevant assurance level/s of the digital ID system?

147. Where the government has not explicitly or implicitly authorised the use of specific digital ID systems for CDD, the regulated entity must first determine, for any digital ID system it is considering adopting, the system's assurance levels.

148. If the government assures, audits or certifies digital ID systems (either directly, or by designating organisations to act on its behalf), regulated entities may rely on these assessments to answer Question Two of the decision process. Similarly, the government may also approve an expert body, domestic or foreign, to test/audit and certify the assurance levels of digital ID systems on which regulated entities may rely. The digital ID systems may be certified as meeting a minimum assurance level, or may have different, increasingly robust assurance levels (either unitary or for each of its components), but the authoritative information should be publicly available.

© 2020 International Compliance Association. All rights reserved.

Extract from the Financial Action Task Force (FATF) Guidance on Digital Identity

149. If the government has neither authorised a digital ID system(s) for use in CDD, nor provided a mechanism to obtain authoritative information on a digital ID system's assurance level/s, regulated entities must determine the reliability, independence of the system themselves by either:

a. performing the assurance assessment themselves, or

b. using audit or certification information on assurance levels by an expert body (albeit not officially government-approved).

150. Where the regulated entity performs the assurance assessment themselves, they should conduct appropriate due diligence on the digital ID system provider, including the governance systems in place, and exercise additional caution.

151. A regulated entity should only use information from another expert body if it has a reasonable basis for concluding that the entity accurately applies appropriate, publicly-disclosed digital ID assurance frameworks and standards. For example, the entity may be approved for similar purposes by another government or may be widely recognised as reliable by appropriate experts in the jurisdiction, region, or internationally.

© 2020 International Compliance Association. All rights reserved.

Extract from the Financial Action Task Force (FATF) Guidance on Digital Identity

Question Three: Is the digital ID system appropriate for the ML/TF risk situation?

152. Once, the regulated entity is satisfied that it knows the assurance levels of the digital ID system (via the processes described under Question Two), it should analyse whether the digital ID system is adequate, in the context of the relevant illicit financing risks, under the FATF's risk-based approach to CDD. In other words, given the assurance level/s, is the digital ID system appropriate for use in customer identification/ verification and ongoing due diligence in light of the potential ML/TF risks associated with the customer, products and services, geographic area of operations, etc.? Regulated entities should analyse whether, given its assurance levels, the digital ID system is adequate, in the context of the relevant illicit financing

153. risks. Depending on the jurisdiction's AML/CFT requirements and available digital ID systems, regulated entities may have the option to select from multiple digital ID systems that have different assurance levels for identity proofing and authentication. In this situation, regulated entities should match the robustness of the system's identity proofing and/or authentication to the type of potential illicit activities and the level of ML/TF risks.

154. In some countries, the government has stipulated a required (unitary) assurance level for standard and or high ML/TF risk situations. Regulated entities may still be able to choose within a range of digital ID system(s) with the required assurance level, or to select varying levels of identity proofing and/ or particular credentials and authenticators offered by the same system. Where this is the case, they should consider the specificities of their ML/TF risks as they relate to identity proofing and authentication in deciding on an option(s). Regulated entities may also have the option to choose appropriate digital ID for lower risk scenarios.

© 2020 International Compliance Association. All rights reserved.

What do we do?

QUALIFICATIONS
View our full
range of courses

TRAINING
View our in-house
training solutions

MEMBERSHIP
Find our more
about membership

EVENTS
View our full
events calendar

© 2021 International Compliance Association. All rights reserved.

Why study with ICA?

It’s the power to make better decisions:
ICA qualifications are not just focused on knowledge delivery but real-world application.

It’s the way to drive effective change:
Provides confidence and credibility.

It’s your path to investing in your future:
Our internationally-recognised qualifications set our professional alumni apart.

It’s you making an impact:
Students understand the impact their role plays in the compliance community, within a global framework that shields society from harm.

© 2021 International Compliance Association. All rights reserved.

ICA Qualifications

"No recertification required; qualification for life"

In association with Alliance Manchester Business School

INTERNATIONAL COMPLIANCE ASSOCIATION

Understanding

New Entrant/Operations

Certificate

- **Length of course:** 4 weeks
- MCQ assessment
- OnDemand online learning

After the course I can:

- actively engage with my processes and procedures
- ask relevant questions
- understand what I'm asked to do and why I need to do it.

Become an Associate Member (AICA)

"Your name" **Cert(AML)**

Enhancing

Analyst/Manager

Specialist Certificate

- **Length of course:** 4 weeks
- MCQ assessment
- OnDemand online learning

After the course I can:

- broaden the projects I am involved in
- ask more specific questions on the topic
- become a catalyst and point of reference on the topic.

Become an Associate Member (AICA)

"Your name" **Spec.Cert(Conduct)**

Applying

Analyst/Officer

Advanced Certificate

- **Length of course:** 6 months
- 1 scenario based MCQ test and 1 written assignment
- Online + Workshops + Tutorials + Assignment preparation

After the course I can:

- identify gaps
- ask exploratory questions
- understand what I need to do, why and how I'm going to do it.

Become an Associate Member (AICA)

"Your name" **Adv.Cert(AML)**

Managing

Manager/Senior Manager

Diploma

- **Length of course:** 9 months
- 3 end of module objective MCQ tests and 2 written assignments
- Online + Workshops + Tutorials + Assignment preparation

After the course I can:

- identify, analyse and resolve gaps
- ask challenging questions
- make reasoned decisions
- support others to do the same.

Become a Professional Member (MICA)

"Your name" **Dip(AML)**

Leading

Senior Manager/Director

Professional Postgraduate Diploma

- **Length of course:** 12 months
- Reflective journal and competency based interview
- Online + Masterclasses

After the course I can:

- evaluate approaches to resolving gaps
- formulate frameworks to questions
- justify and critque decisions
- lead others to do the same.

Become a Fellow Member (FICA)

"Your name" **Prof.PgDip(AML)**

MANCHESTER 1824
The University of Manchester
Alliance Manchester Business School

Trustpilot

64 NPS

Rated Excellent across 40,000 annual learners, across 850+ workshops and 150 countries

www.int-comp.org

ICAB10050

Solutions for your firm

Corporate Membership

ICA qualifications delivered in-house & tailored learning solutions

ISO Certifications Quality Management Anti Bribery & Corruption and Compliance Systems

© 2022 International Compliance Association. All rights reserved.

Thank you

www.int-comp.org

The information that is provided is in confidence and may not be disclosed to any third party or used for any other purpose without the express written permission of the International Compliance Association. Whilst every effort has been made to ensure accuracy, International Compliance Association cannot be held responsible in any way for consequences arising from the information given. No formal decisions should be taken on the basis of information provided without reference to specialist advice.

© 2020 International Compliance Association. All rights reserved.