

Introduction to Compliance and Compliance Risk

What is Compliance?



Compliance means to obey an order, rule, or request, such as a corporate policy, international standard or law. This includes following the internal policies and procedures of KBZ MS.



Making sure that all staff members comply with our policies and procedures is the Compliance Department. It is their job to make sure that everyone knows the rules and sticks to them.

Compliance is a good thing!

Following the rules helps to ensure that everyone is treated fairly and consistently.

Compliance is important for:



1. Protecting the company and employees



2. Improving efficiency and productivity

3. Setting clear requirements for everyone to follow



What are the risks?

Risk is the likelihood of consequences.

The Compliance Department helps to manage risk by highlighting the rules, monitoring that everyone follows them and helps to assess risk and compliance using software tools and expertise.

Not complying with the rules is known as Compliance Risk and its effects can be very serious. Consequences can include legal penalties, financial and material losses, loss of job(s), loss of license and damage to reputation. When it comes to compliance and compliance risk, everyone in the company has a part to play.



Company
Employees

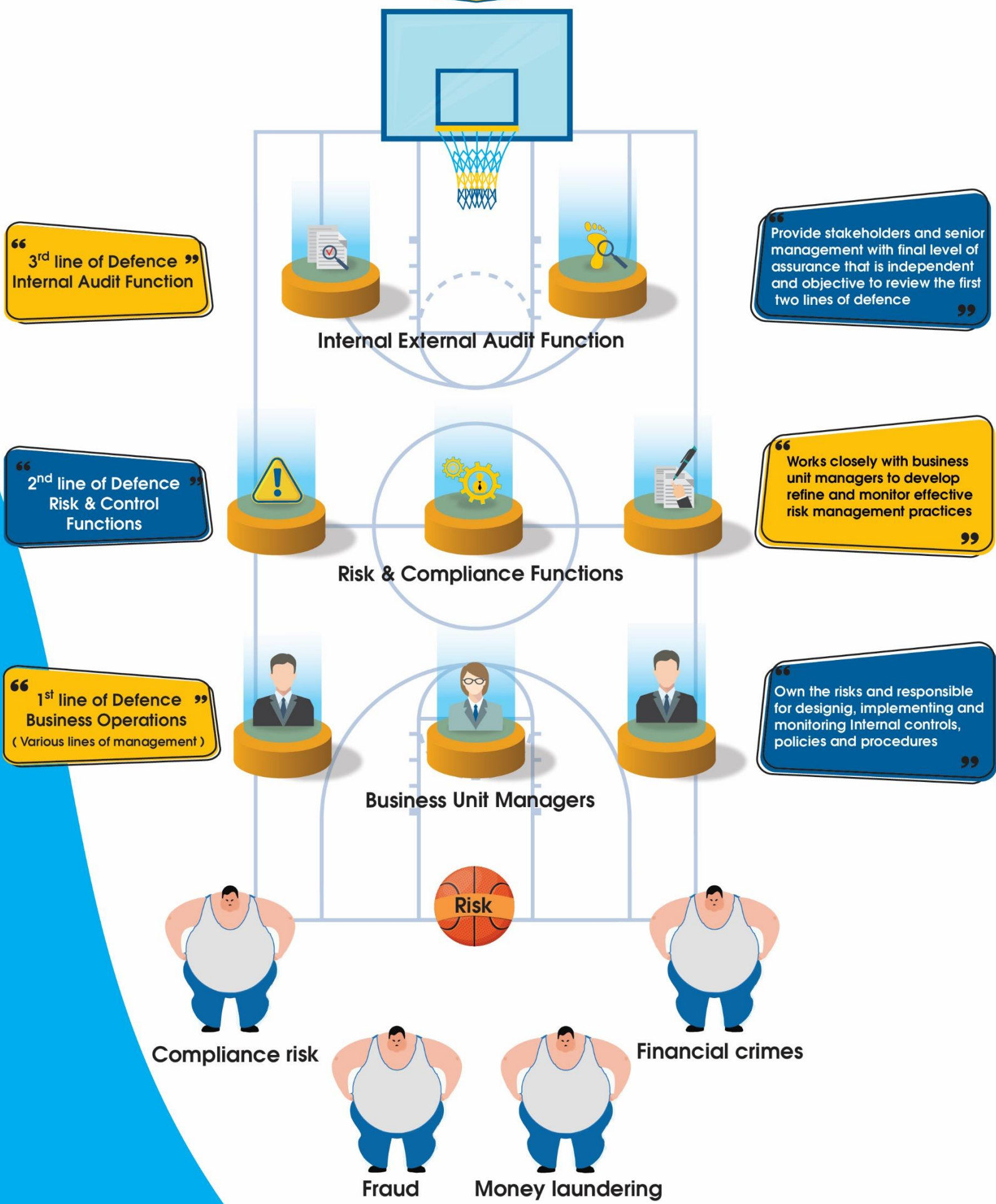
DILIGENCE

Supplier & Distributor Network
International Relationship
Expanding Markets
Better Governance
Better Regulatory Relationship
Competitive Edge
Market Share
Contract obligations and honouring
Relevant laws and regulations
Legal Ventures and operations
Ethical Works
Reputation Risk management
Free of economic crimes
Stringent Internal Guide lines

TRUST

Customers
Suppliers
Representatives
Connected Groups
Business Partners

Company Reputation



Introduction to Compliance and Compliance Risk

Case Study: Standard Chartered Bank

In April 2019, Standard Chartered Bank was fined USD 1.1 billion for violating US sanctions against Iran and other countries as well as over inadequate financial crime controls. A USD 133 million fine was specifically imposed for control and compliance failures. The penalties date back to violations from before 2014. As part of the settlement Standard Chartered was also required to improve processes & procedures with an independent consultant overseeing remediation efforts to ensure compliance.

The fines rank amongst the most severe imposed for sanctions violations, which occurred not long after settlement for similar charges in 2012.

Investigations by US and UK authorities found "serious and sustained" shortcoming in Standard Chartered's anti-money laundering controls.

Violations such as these "undermine the integrity of the financial system and harms national security by deliberately providing Iranians (and terrorist-linked organisations) with access to legitimate international financial markets" according to US authorities.

One former banker from the Dubai branch pleaded guilty to conspiracy to violate sanctions. An Iranian client was similarly charged. The bank's Chief Executive, was compelled to make a series of reassuring statements to mitigate the damage to the organization's 160-year reputation.



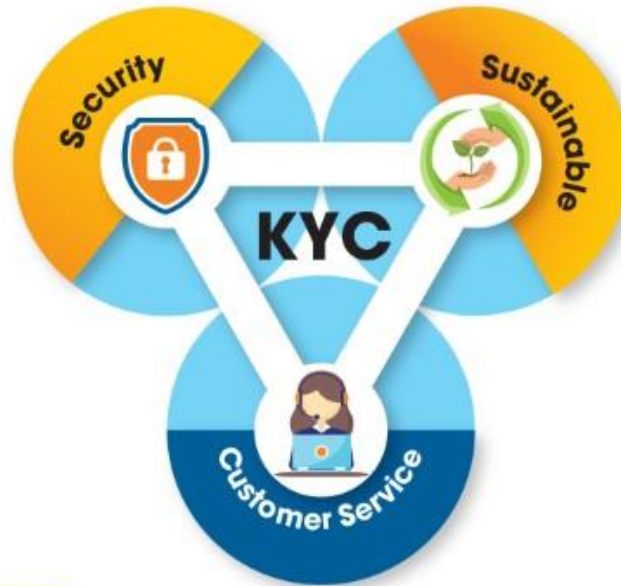
What is Know Your Customer (KYC)?

Know Your Customer (KYC) is the process of verifying the identity of the customer and assessing their suitability, along with the potential risk of illegal intentions towards the business relationship.

The company obtains information about the identity, address, beneficial ownership, source of funds and nature of the business of the customer in order to ensure that KBZ MS services are not misused.

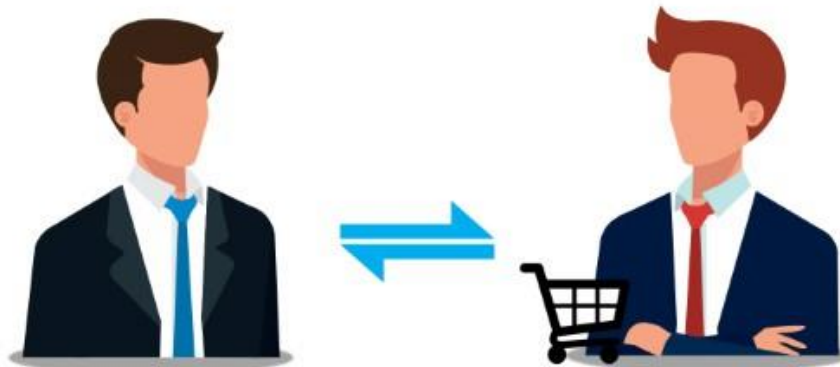
KYC details should be updated from time to time to ensure that KBZ MS continues to offer the correct services to the customer.

The same information can also be used to help safeguard a customer's account by flagging any unusual activities, which might not align with the customer's known profile.



KYC Protects Everyone!

The KYC process is designed to prevent KBZ MS being used (intentionally or unintentionally) for criminal activities such as money laundering, terrorism financing, identity theft and financial fraud. KYC allows us to protect ourselves by doing business legally and with legitimate entities, and it also protects the individuals who might otherwise be harmed by financial crime, including our customers.



The more you know your customer,
the more you can manage the risk
to doing business with them and
the more you can provide an efficient
and customized service.

The more the company knows about you,
the more you sure financial safety.

How does it work?

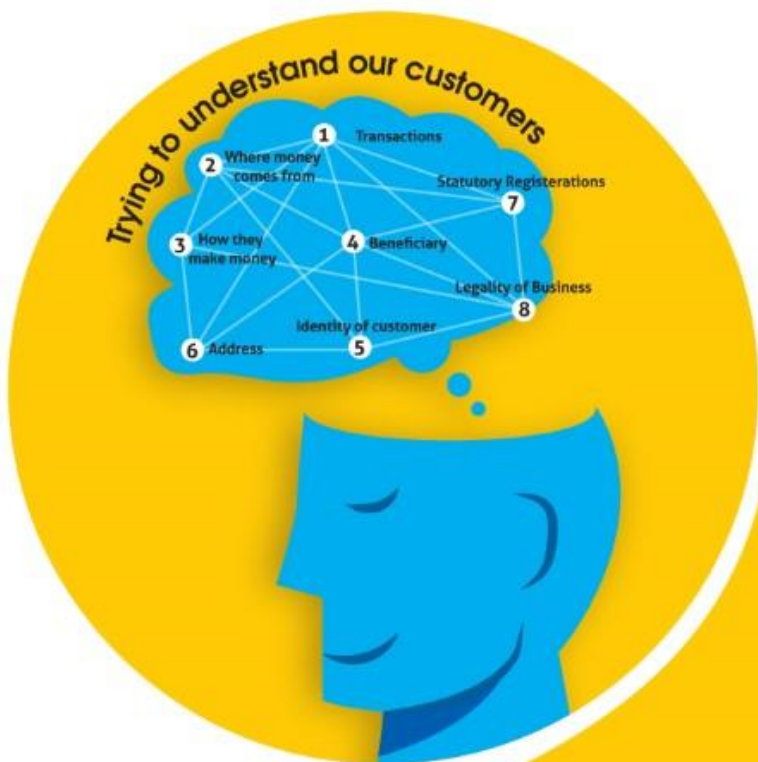
KYC starts with the process of collecting basic information about customers, ideally using electronic identity verification to ensure the information is true and accurate.

Information collected includes:

- Names
- Addresses
- Date of Birth
- Occupation/ Type of Business
- Source of funds
- Beneficiaries
- Statutory Registration/ Legality of Business
- Transactions

Once this basic data is collected, it is scrutinized to determine the risk of customers being involved in potential corruption, on a list of sanctions, suspected criminals, or at a high risk of partaking in bribery or money laundering.

This client profile can also be used to assess the customer's needs and to detect suspicious transactions that do not match the customer profile.



Case Study

Daniel Fernandes Rojo Filho, a Brazilian national and self-proclaimed billionaire living in Florida, was the owner of 17 bank accounts opened at prestigious banks such as Citigroup, JP Morgan Chase and Wells Fargo. He made no attempts to hide his identity, opening the accounts under his own name and using his original signature. His company name, DFRF Enterprises, was derived from his initials. DFRF Enterprises offered investors a perpetual 15% return on investments, reportedly secured by gold mining operations in Brazil and Africa and a credit line in Switzerland. The company soon raised over USD 15 million from investors. But there was a problem: there were no gold mines, there was no Swiss credit line and the investors in DFRF Enterprises were victims of a ponzi scheme by a known fraudster. In 2015 U.S authorities brought DFRF to court for alleged conspiracy involving drug trafficking, money laundering and managing a Ponzi scheme. The banks somehow missed or ignored historical data and public records proving a criminal history dating back many years and allowed Rojo Filho to gain access to the financial systems once again. He didn't even need to use a fake name to secure the accounts. This incident proves how much damage a single individual can do if given access to the financial markets and demonstrates why it is necessary to follow KYC and due diligence processes.

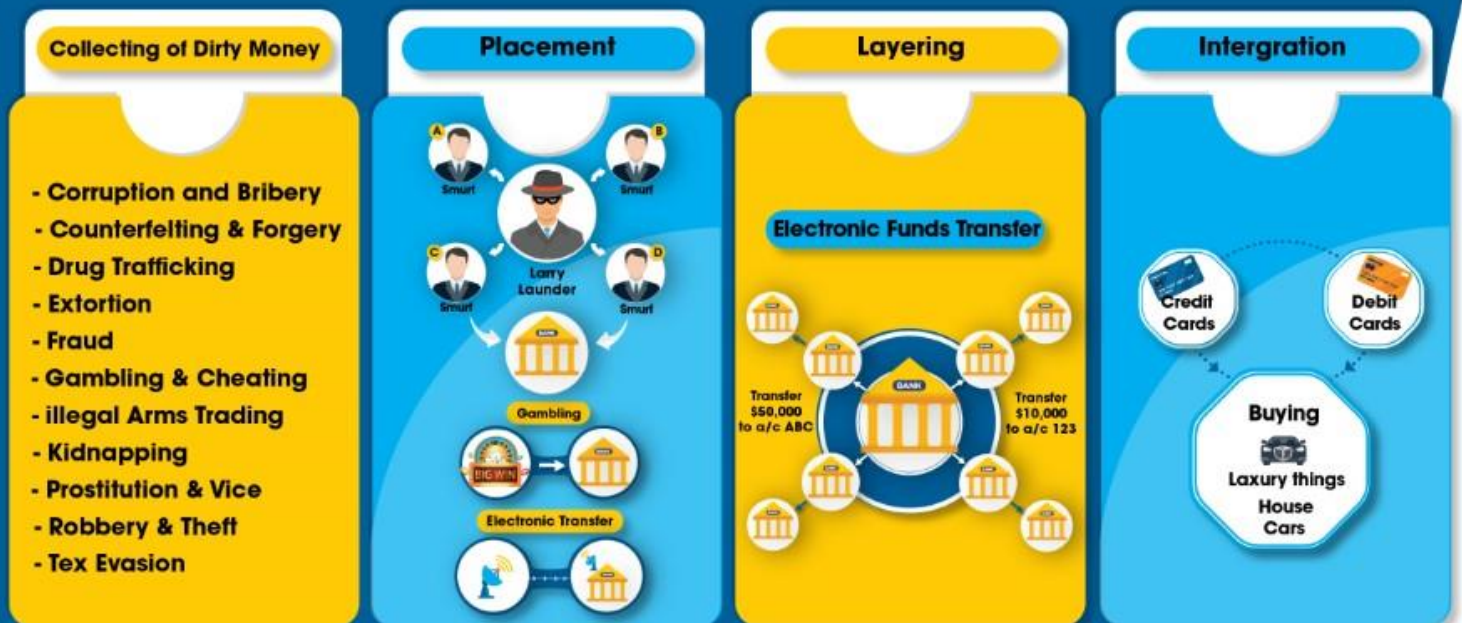


What is Money Laundering?

Money Laundering is the process by which illegally obtained funds and assets are converted into legitimate funds and assets. It involves the conversion of profits from illegal activities into financial assets which appear to have legitimate origins.

Simple Bribe and Money Laundering Transaction

How does Money Laundering Work?



What is Anti-Money Laundering?

Anti-Money Laundering (AML) is a set of laws, regulations and procedures intended to prevent criminals for disguising illegally obtained funds as legitimate income. Companies that are found to be complicit in money laundering activities face stiff penalties, suffer from reputational risk and are potentially subject to criminal prosecution.

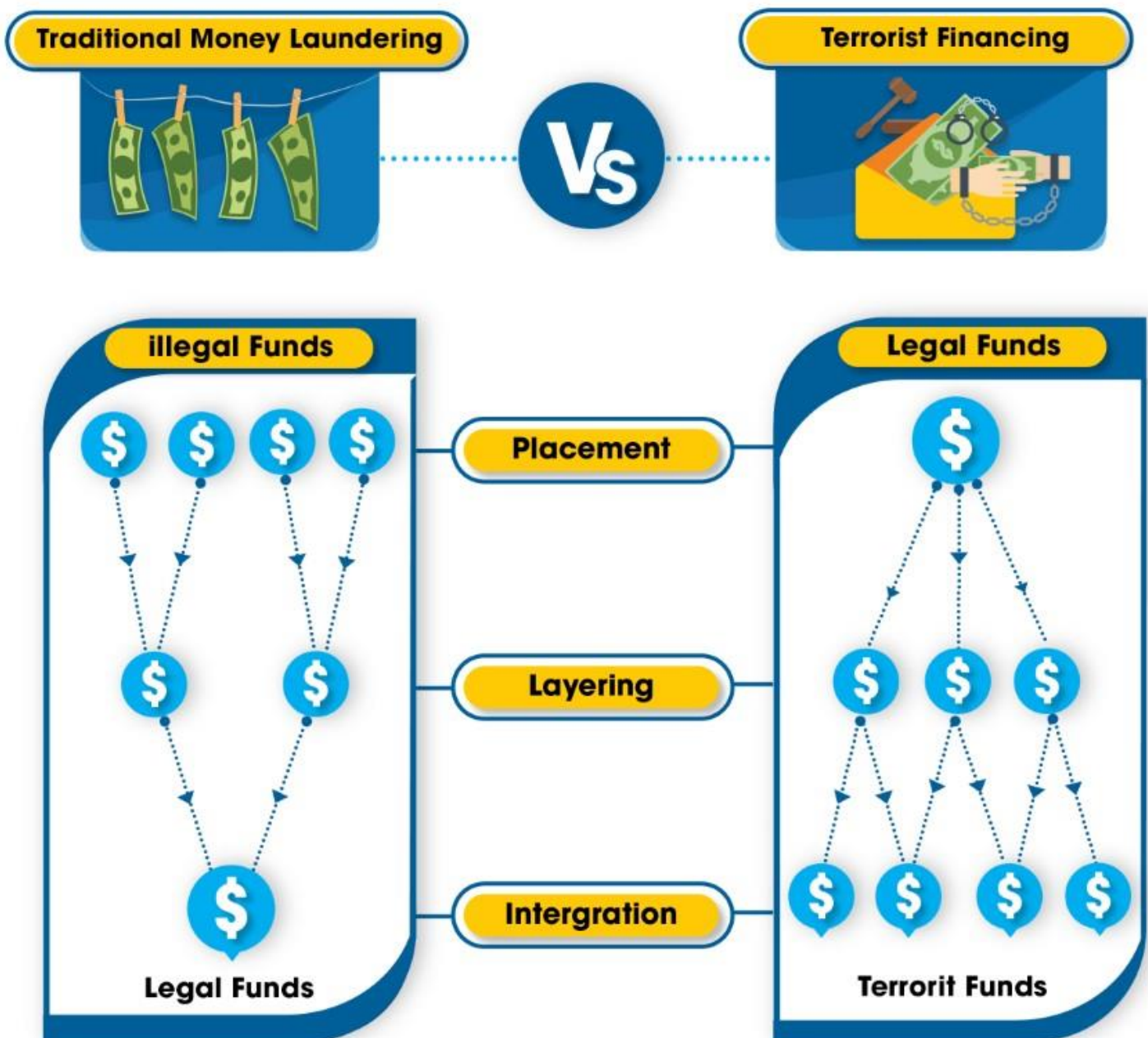


Money Laundering & Terrorist Financing

Besides for benefiting criminal syndicates, money laundering techniques are also used to fund potential terrorist activities.

Terrorist Financing may also involve funds raised from legitimate sources, such as personal donations and profits from businesses and charitable organizations, as well as from criminal sources.

Disrupting and preventing their financial flows and transactions is one of the most effective ways of fighting terrorism.



Case Study

Big Four accounting firm EY is accused of covering up transactions which involved a crime gang laundering British drug money. The investigation implies the Big Four firm failed in reporting suspicious activity led by the gold refinery Kaloti in Dubai. The crime gang was convicted in 2017, but its money laundering approach has just been revealed.

In 2013, Kaloti, 40 per cent of whose business, amounting to \$5.2billion, was conducted in cash had received large quantities of gold coated in silver from Morocco. Kaloti had also accepted around two tons of gold from walk-in customers without carrying out proper know-your-client tests, and had also bought gold from Sudan, an armed conflict zone. All suspicious activities, indicating potential money laundering, which EY is accused of watering down in their official reports.

The story started in Britain, in which a drug dealing boss received hundreds of thousands of pounds in cash that needed to be laundered. The drug money was handed over to an airport cleaner in the UK, who transported the money to Paris where it was collected by an ambulance driver who aggregated money from various other money mules. The money was then split into smaller packages and picked up by middle aged women and transported to Belgium where it was exchanged for gold. The gold finally reached Dubai via Amsterdam, where it was sold back into cash and transferred to bank accounts across the world- making the money untraceable.

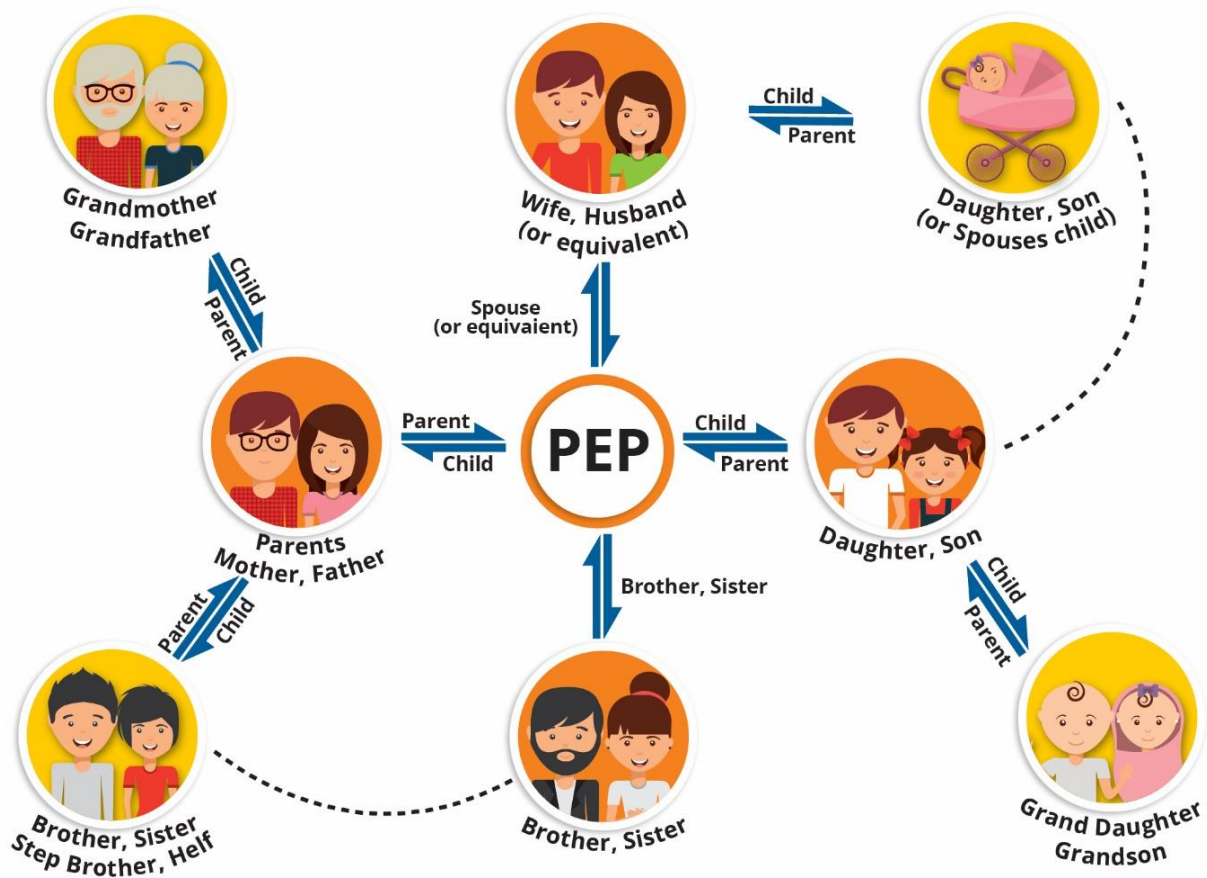
This story highlights the lengths that criminals will go to to hide their illicit gains and reemphasizes the importance of following international AML best practices.



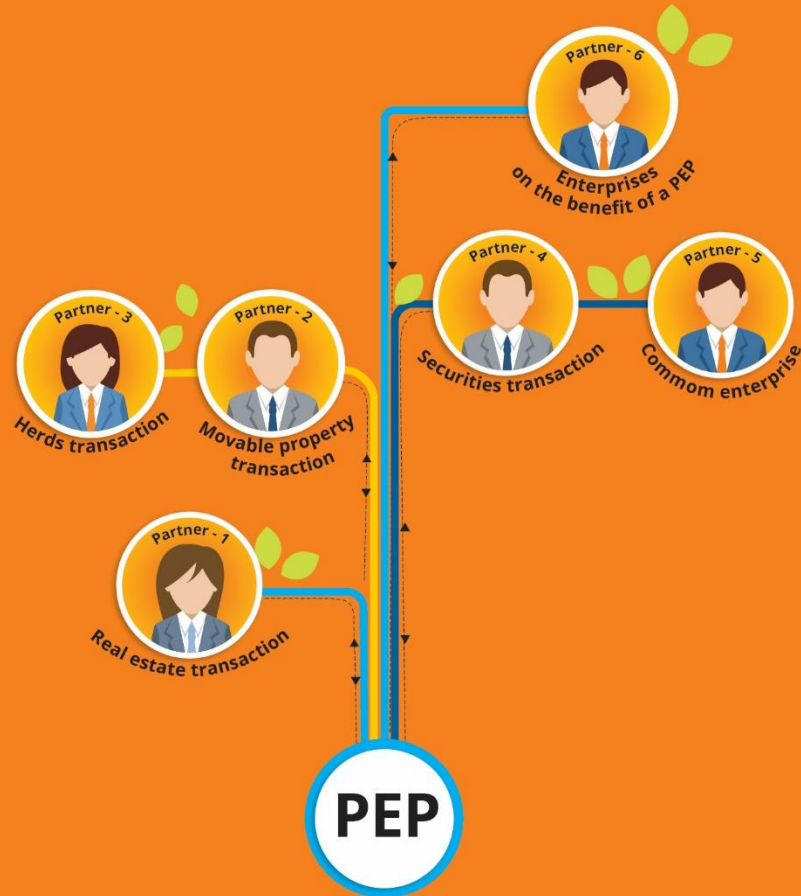
What is Politically Exposed Person (PEP)?

In financial regulation, a politically exposed person (PEP) is an individual who has been entrusted with a prominent public function. Although there is no universal definition of PEPs, the Financial Action Task Force (FATF) defines a PEP as:

- 1 - A current or former senior official in the executive, legislative, administrative, military, or judicial branch of a government (elected or not)
- 2 - A senior official of a major political party
- 3 - A senior executive of a government-owned commercial enterprise, being a corporation, business or other entity formed by or for the benefit of any such individual
- 4 - An immediate family member of such individual; meaning a spouse, parents, siblings, children, and the spouse's parents or siblings
- 5 - Any individual publicly known (or actually known by the relevant financial institution) to be a close personal or professional associate.



PEP Family Members



Persons closely related to a PEP

Identifying PEPs

- Based on their occupation, their authority and their network.

How to identify National and International PEPs

- Through the KYC process, all customers must fill out their name and occupation.
- Through suspicious transactions like unusual dealing patterns and abnormal activities. For instance in the insurance industry, if a customer buys insurance policies at a higher value than his/her stated occupation salary, this could be considered suspicious.

Enhanced Procedures and Controls

Procedures and controls for PEPs are still developing but often include forms of Customer Due Diligence.

Customer Due Diligence (CDD)

Customer Due Diligence (CDD) is a complimentary process to Know Your Customer (KYC) that involves verifying transactions. KBZ MS conducts due diligence at appropriate times on insurance transactions of existing and new policyholders, based on the products, services and customer risk categorization.



Case Study (Former President Park Geun Hye)

In 2016, a high-profile corruption case ensnared disgraced former president Park Geun-hye, daughter of ex-military leader Park Chung-hee, her controversial friend Choi Soo-sil (daughter of pseudo-Christian cult leader Choi Tae-min) and Samsung Group heir Lee Jae-yong. Lee Jae-yong, the son of Samsung Group's Chairman, is also the grandson of Samsung founder Lee Byung-chul. Since his father's heart attack in 2014, he has been considered de facto boss of the entire Samsung Group.

Following the assassination of Park's mother in 1974 and her father in 1979, Choi Soo-sil, daughter of "the Korean Rasputin", became a close family friend and Park's advisor when she became President.

Choi was found to have used her presidential connections to pressure conglomerates - including electronics giant Samsung - for millions of dollars in donations to two non-profit foundations she controlled.

Samsung was accused of paying 43bn won (USD 37.7 million) to two non-profit foundations operated by Choi Soon-sil in exchange for political support. More specifically, the favors were alleged to include backing for a controversial Samsung merger which paved the way for Lee to become eventual head of the conglomerate, a deal that needed support from the government-run national pension fund.

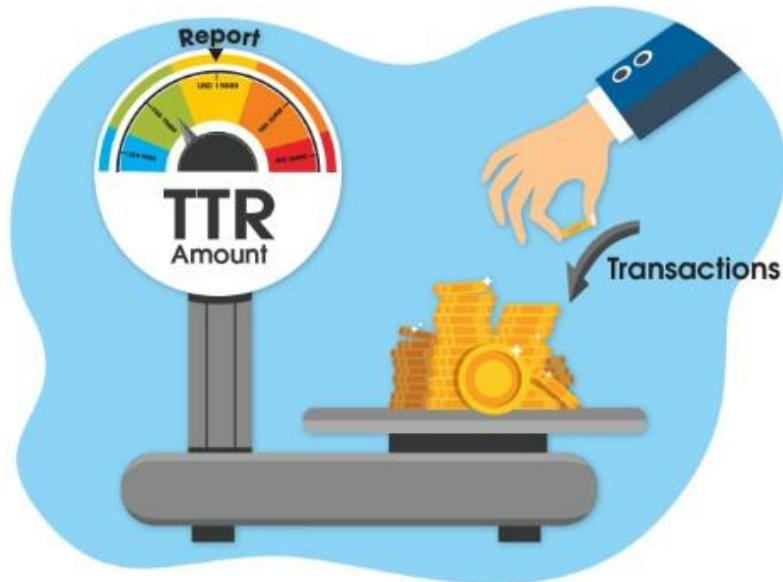
Park meanwhile was accused of colluding with Choi and giving her unauthorised access to state documents. After losing her presidential immunity, she was charged with bribery, abusing state power and leaking state secrets.

On 9 December 2016, the National Assembly impeached Park on charges related to influence peddling by her top aide, Choi Soon-sil. The impeachment was unanimously upheld by the Constitutional Court on 10 March 2017, thereby removing Park from office and on 6 April 2018, South Korean courts sentenced Park to 24 years in prison. Further charges were added later.

Lee Jae-yong was arrested in February 2017. In August 2017, a court convicted him over payments made to Choi's foundations, as well as for giving a horse and several million dollars to assist the equestrian career of Choi's daughter. Lee was also found guilty of hiding assets overseas, concealing criminal proceeds, and perjury. He was sentenced to prison for five years. However in February 2018, that sentence was halved when Seoul High Court agreed that Samsung merely allowed Choi Soon-sil's daughter to use the horses and it did not transfer ownership to her and decided to suspend the jail term, meaning he was free to go.

In February 2018, Choi was sentenced to 20 years in jail for corruption, influence-peddling and abuse of power. She was earlier found guilty of using her position to solicit favours for her daughter, including 3.6 billion won that Samsung sent to Choi's German-based firm to sponsor her daughter Chung Yu-ra's equestrian training and another 3.4 billion won used to buy the three expensive horses for her to use.

What is Threshold Transaction Report (TTR)?



Threshold Transaction Report (TTR) is a report that financial institutions, like KBZ MS, are required to submit to the Myanmar Financial Intelligence Unit about designated products, such as deposits, withdrawals, currency exchange and other payments and transfers. In Myanmar, this applies to transactions of US Dollar currency or equivalent to Myanmar Currency Kyat:

The courage to do the right thing!



What is a Suspicious Transaction?

Suspicious transactions are transactions which to a person acting in good faith:

- Gives rise to reasonable ground for suspicion that it may involve the proceeds of crimes
- Appears to be made in unusual circumstances or overly complicated
- Appears to have no economic rationale or bona fide purpose
- Providing misleading information or hard to verify information
- Large cash withdrawals from dormant accounts
- Sudden increase of cash deposits without justification
- Lavish lifestyle that do not match income sources
- Substantial increase in turnover in dormant account
- Receipt or payment of large cash sums with no obvious purpose or relationship to account holder
- Reluctance to provide normal information when opening an account or providing fictitious information

What is Suspicious Transaction Report (STR)?

Suspicious Transaction Report is a report submitted to Myanmar Financial Intelligence Unit about suspicious or potentially suspicious activities to the proceeds of illegal activities such as money laundering and terrorist financing.



Importance of TTR and STR

It is to identify illegal activity including tax fraud, money laundering, terrorist financing and other financial fraud.

Do

- When a suspicious activity is detected, it is required to confirm and submit the STR
- Take the time to gather more evidence (if required) to support the document
- It is necessary to report related authorities if you have reasonable ground to be suspicious

Don't

- Do not inform or discuss with third-parties such as media organizations, friends including family members as it is legally forbidden and confidential information
- Do not take any actions toward customers even if you have suspicions