Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

AML & ESG Executive Training 2025:

New Format Compliance Training Workshop on AML and ESG in Kenya

30 OCT — 01 NOV 2025

Empowering through practice

Who we are - AML Certification Centre

AML Certification Centre
AML Certification Centre is an internationally recognised and accredited European certification and training institution, building a global community of professionals in the AFC field.

What We Solve
Growing shortage of well-trained AFC specialists, limited access to comprehensive training, stricter regulations, and a rising number of misconduct cases.

Our Background
Backed by decades of experience and a team of industry-leading experts-practitioners, we apply innovative methods to develop practical skills via our user-friendly platform.

Our Mission

What is driving us forward?

While financial crime has many drivers, profit remains the most consistent and powerful among them. By targeting and dismantling these profit-driven motives, we strike at the heart of what drives these crimes.

Education is where this journey begins.

AGENDA

- Introduction & Opening Keynotes
- What Every Financial Institution Must Know About Kenya’s AML Laws
- Dirty Money Exposed: How Organised Crime Targets the Financial System
- Detecting Criminal Activity Early: Key Financial Crime Typologies in 2025
- How the Financial Sector Can Interrupt the Flow of Criminal Funds: Real Cases & Tactics
- Avoiding Regulator Red Flags: Best Practice in STRs & Reporting
- Mastering CDD & BO: Getting Risk-Rated KYC Right

AML Certification Centre
By Crence

Certification Centre
By Crence

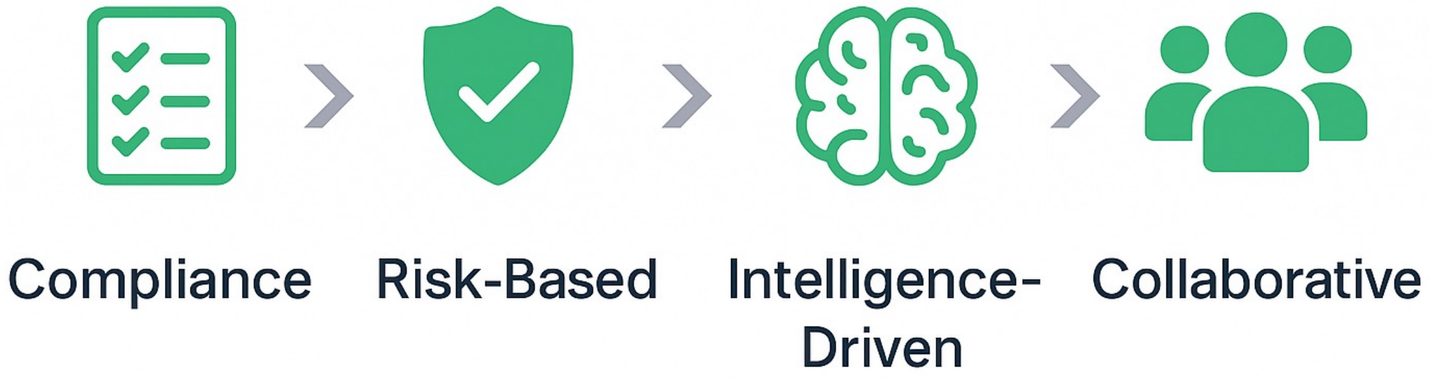
Purpose of the Training

To strengthen the ability of compliance professionals to identify, analyse, and disrupt financial crime operations through real-world case understanding and cross-sector collaboration.

The Global AML Shift

Certification Centre
By Crence

From rule-based compliance to risk-driven intelligence:



- Global regulators are moving from tick-box supervision to outcome-based evaluation.
- The EU AML Package and AMLA, the UK's post-Brexit reforms, and FATF's enhanced focus all prioritise effectiveness over paperwork.
- Financial institutions are expected to prove understanding, not just procedures.
- Data, behavioural analytics, and cross-border cooperation are now at the centre of AML strategy.
- The new expectation: "Detect early, act fast, document everything."

AML Certification Centre
By Crence

Keynote Speech:

Kenya-Estonia Cooperation in AML

Kadri Humal-Ayal
Honorary Consul
of the Republic of Estonia

Certification Centre
By Crence

What Every Financial Institution Must Know About Kenya's AML Laws

Robert Muoka

Senior Partner, T.M.M
Partners Advocates

Executive Summary

The 2025 Amendment Act strengthens Kenya’s AML/CFT/CPF framework.

Key changes:

- Expanded regulated entities
- Enhanced supervisory powers
- Stricter penalties
- Clearer institutional mandates

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Key Institutions & Strengthened Mandates

The amendments reinforce the FRC, ARA, and multiple sectoral regulators.

Institutions:

- Financial Reporting Centre (FRC)
- Assets Recovery Agency (ARA)
- Sectoral Supervisory & Self-Regulatory Bodies

Financial Reporting Centre (FRC)

Mandate: Collect, analyze, and share financial intelligence.

New Powers:

- Risk-based supervision (Section 36D)
- Periodic reviews of institutional risk
- Expanded investigative authority via ARA collaboration

Assets Recovery Agency (ARA)

Mandate: Investigate, trace, freeze, and recover proceeds of crime.

Key Changes:

- Head renamed to 'Director-General'
- Establishment of ARA Advisory Board
- Full police powers for investigators under multiple sections

Supervisory & Self-Regulatory Bodies

Expanded oversight across multiple sectors:

- Betting Control and Licensing Board (Gaming)
- Retirement Benefits Authority (Pensions)
- Director of Mines (Minerals)
- SASRA (SACCOs)
- ICPAK (Accountants)
- Estate Agents Board (Real Estate)
- PBO Authority (NGOs/Charities)

New Powers of Regulators

All regulators can now:

- Vet senior management & shareholders
- Conduct inspections & surveillance
- Compel production of information
- Impose monetary/civil sanctions
- Issue guidelines & directives

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

Expanded Definition of Reporting Institutions

- Dealers in Precious Stones & Metals now explicitly covered
- Mandatory reporting of cash transactions ≥ USD 15,000
- Public Benefit Organizations (PBOs) under FRC oversight for TF risk

Stricter Penalties & Sanctions

Non-compliance:

- Up to 7 years imprisonment or KES 10M fine (individuals)
- Up to KES 20M fine (corporates)

Terrorism financing offences: Up to 20 years or KES 20M

Sectoral penalties: KES 5M (legal persons) / KES 1M (individuals)

Certification Centre By Crence

T.M.M & PARTNERS ADVOCATES

LEGAL EXPERTISE, PERSONALIZED SERVICE

Mandatory Risk-Based Approach (RBA)

Institutions and supervisors must apply a risk-based approach.

- Tailor AML/CFT programs to specific risk profiles
- Document and periodically review risk assessments
- Expect supervision intensity based on institutional risk

Conclusion & Action Points

Immediate steps:

- Update AML/CFT/CPF policies
- Conduct fresh risk assessment
- Train staff on new obligations
- Engage with your supervisory body

Kenya’s strengthened AML framework makes compliance a core operational priority.

Certification Centre By Crence × T.M.M & PARTNERS ADVOCATES
LEGAL EXPERTISE, PERSONALIZED SERVICE

AML Certification Centre By Crence

Dirty Money Exposed:

How Organised Crime Targets the Financial System

Col. ret. Igoris Krzeckovskis

International Anti-Financial Crime Expert

Certification Centre
By Crence

Behind a luxury car and offshore company, there’s sometimes a story of someone trying not to be found

Understanding organised crime patterns is crucial for financial institutions and law enforcement alike

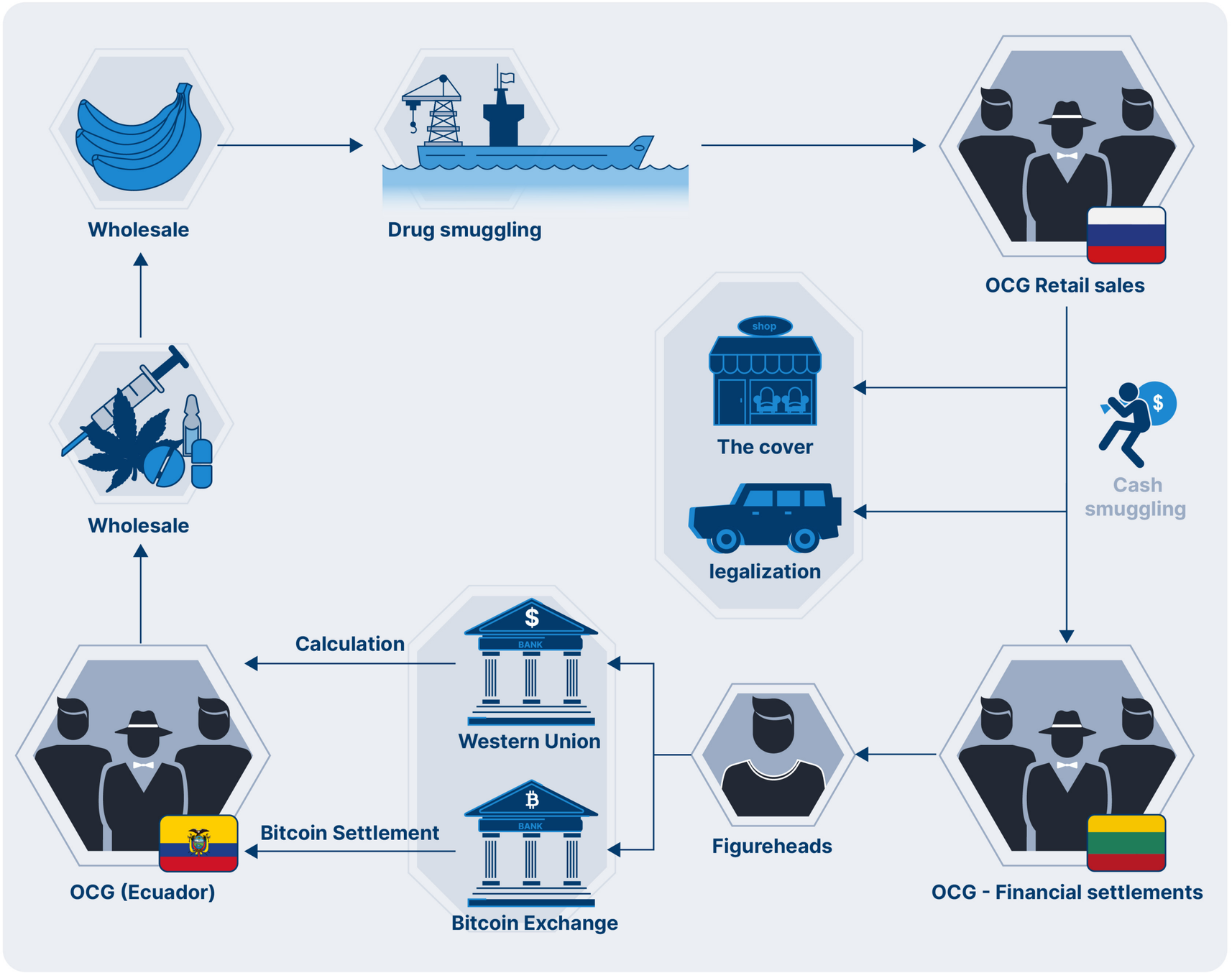
Certification Centre
By Crence

What is a Predicate Offence?

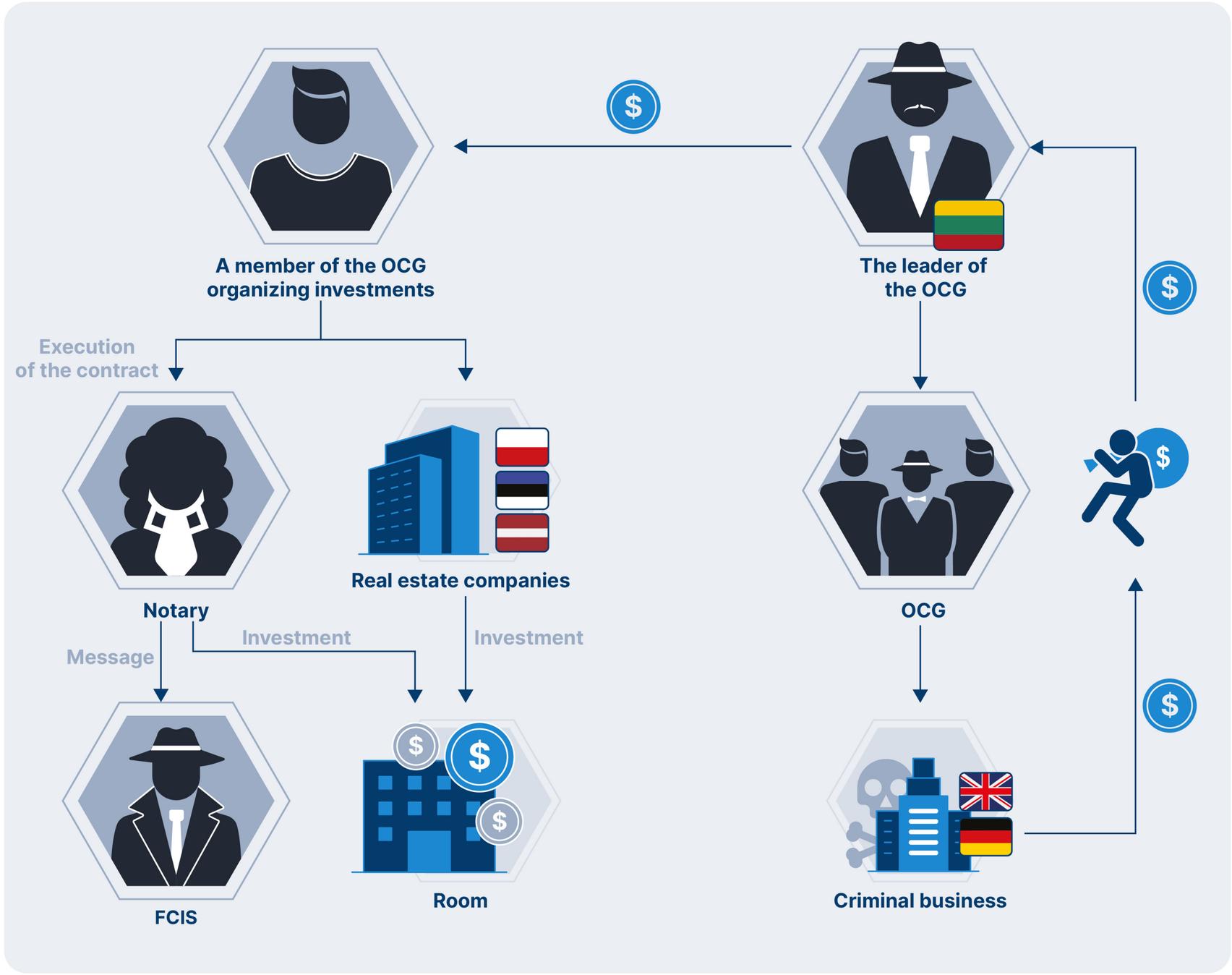
“The 3 Stages of Money Laundering” Model

Placement Layering Integration

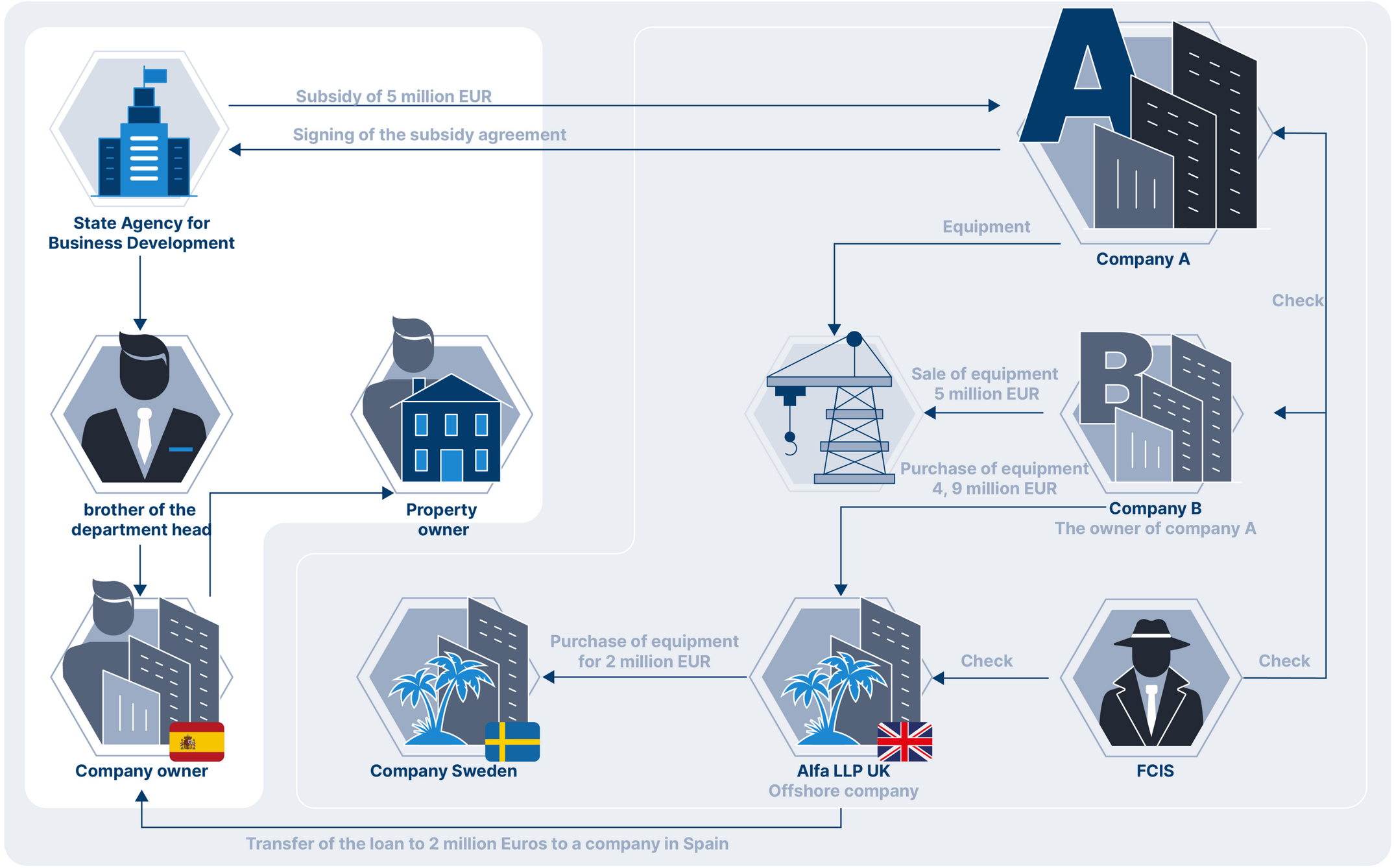
Drug trafficking and money laundering



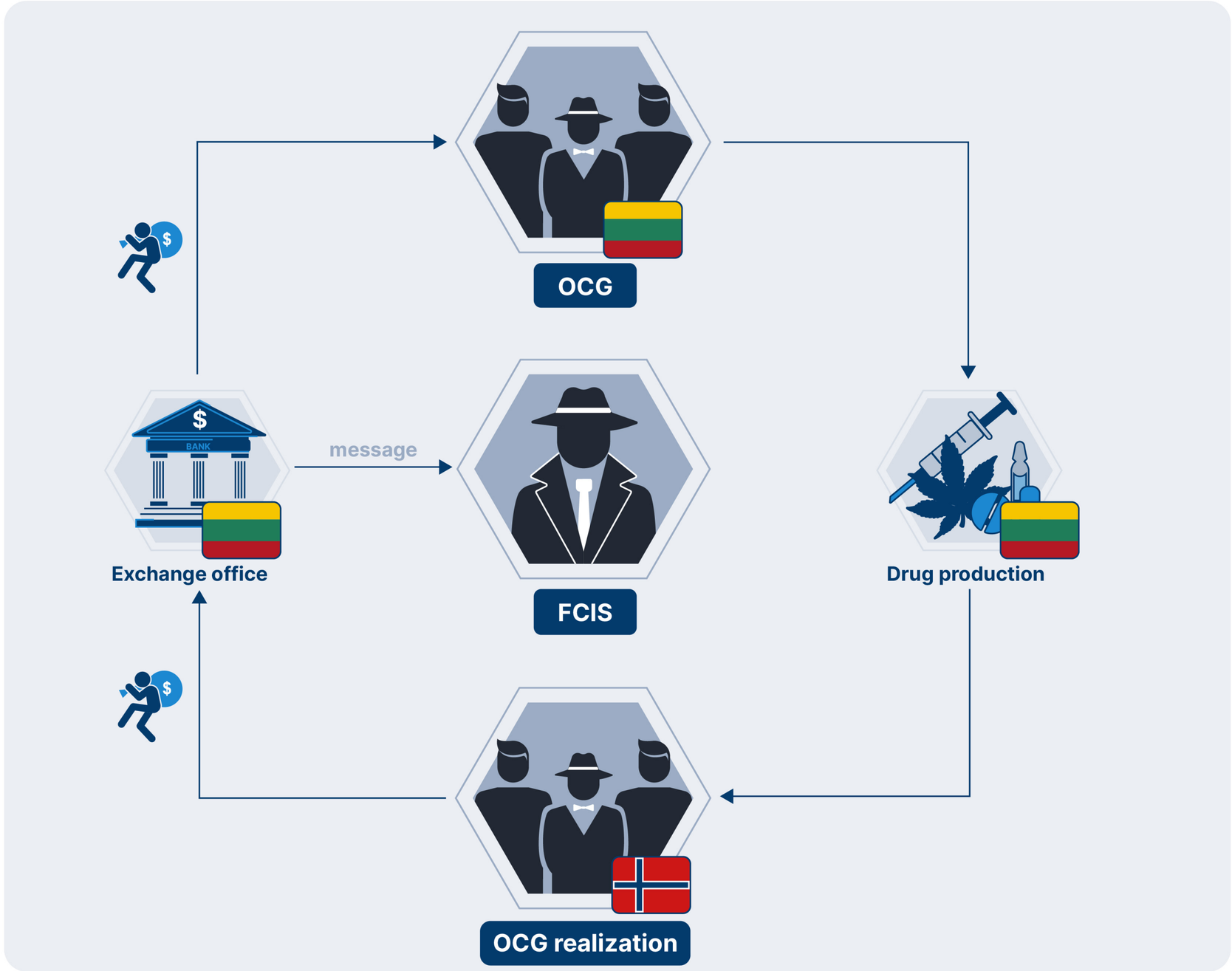
Investment of criminal assets in real estate

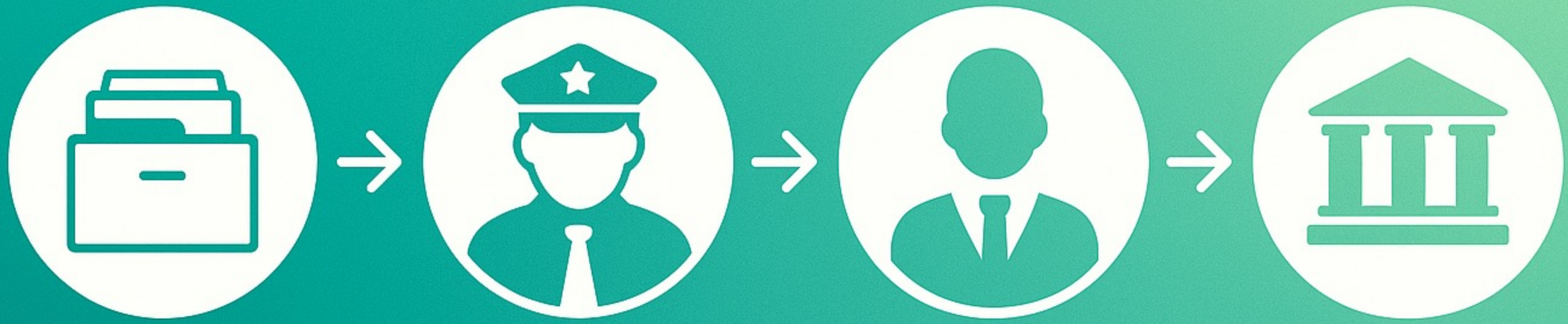


Fraud with government subsidies, corruption and money laundering



Exchange of cash received as a result of the sale of synthetic drugs




FIU
Law enforcement
Prosecutors
Courts

Certification Centre
By Crence

Detecting Criminal Activity Early:

Key Financial Crime Typologies 2025

Andrei Sribny

CEO, AML Certification Centre

Certification Centre
By Crence

> **The sooner we detect, the less we investigate**

Understanding typologies

Certification Centre
By Crence

Typologies = Patterns of criminal behaviour that reveal intent.
Typologies evolve slowly. But methods and channels rapidly.

- Based on real investigations, STRs, and intelligence sharing.
- Developed by FATF, FIUs, and law enforcement to identify recurring criminal methods.
- Each typology shows how crime works, not just what it is — helping detect intent early.

> *Typologies bridge intelligence and practice — turning investigations into prevention tools.*

Why typologies are stable?

1

Human and economic motives don’t change: greed, concealment, profit, control.

2

The structural opportunities — like trade, corporate vehicles, intermediaries — remain the same.

Therefore, core typologies have remained constant for decades.

Certification Centre
By Crence

Use of Stablecoins by Criminals

01

Certification Centre
By Crence

- Stablecoins are now widely used in on-chain illicit finance.
- Involvement of DPRK actors, terrorist financiers, and scammers.
- Use of dormant accounts and privacy tools to obscure transactions.

Example: DPRK-linked hackers laundered stolen funds using Tether on multiple exchanges.

Example: Romance scammer used USDT wallets to cash out victim proceeds anonymously.

Certification Centre
By Crence

DeFi Platforms as Crime Enablers

02

- **Criminals exploit DeFi's lack of central control for money laundering.**
- **Difficult to regulate due to unclear governance.**

Example: Fraudsters used a DeFi yield farming platform to move illicit funds from rug-pulls.

Example: Anonymous mixing protocols on DeFi used to hide ransomware proceeds.

Scam-as-a-Service Ecosystems

03

Certification Centre
By Crence

Professional tools for running crypto scams sold on dark web.

AI chatbots and deepfakes used in fraud campaigns.

Example: Pig butchering scam run with scripts, fake trading platforms, and Telegram bots.

Example: Victims lured into fake investment schemes by realistic AI avatars.

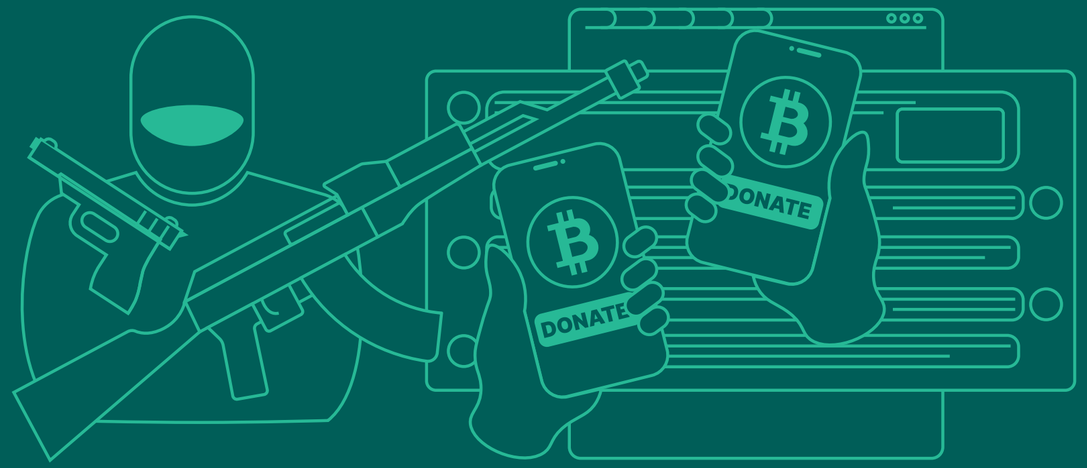
Terrorist Financing with Virtual Assets

04

Certification Centre
By Crence

Terrorists use VAs for micro-financing and propaganda.

Privacy coins and social media-based fundraising increasingly common.



Example: ISIL-K supporters use Monero and Telegram for global donations.

Example: Lone actors use crypto-crowdfunding with pseudonymous wallets.

Offshore and Unlicensed VASPs

05

Certification Centre
By Crence

Jurisdictions with weak AML used to route illicit crypto flows.

Evasion of Travel Rule by transferring between non-compliant VASPs.

Example: Exchange in low-regulation country used to cash out ransomware funds.

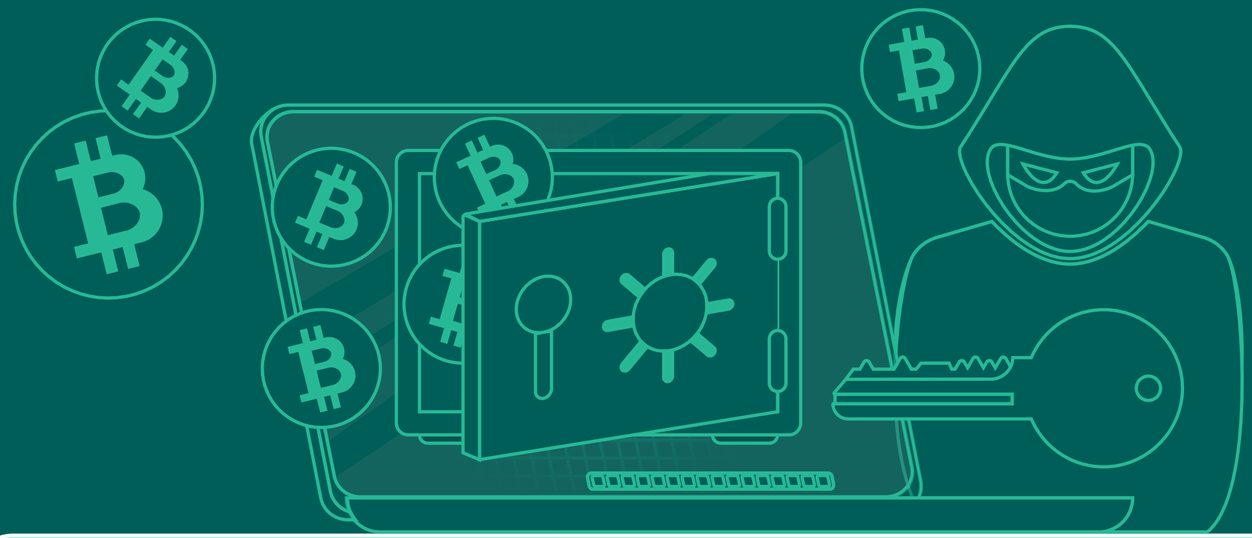
Example: Criminals hopping between VASPs to avoid KYC enforcement.

Crypto-enabled Fraud and Theft

06

Certification Centre
By Crence

- Fraud disguised as legitimate crypto projects.
- Nation-state actors behind major VA thefts.



Example: Fake ICO raised millions before disappearing with funds.
Example: DPRK's 2025 hack of centralised wallet provider – largest crypto theft to date.

Risk from Unhosted Wallets

07

Certification Centre
By Crence

Used to store and transfer funds outside regulated systems.

Difficult to trace without VASP involvement.

Example: Funds moved from exchange to private wallet, then mixed and withdrawn as cash.

Example: Use of QR codes and cold wallets in illicit cash-for-crypto schemes.

Geographic Trends and Regional Risks

08

Certification Centre
By Crence

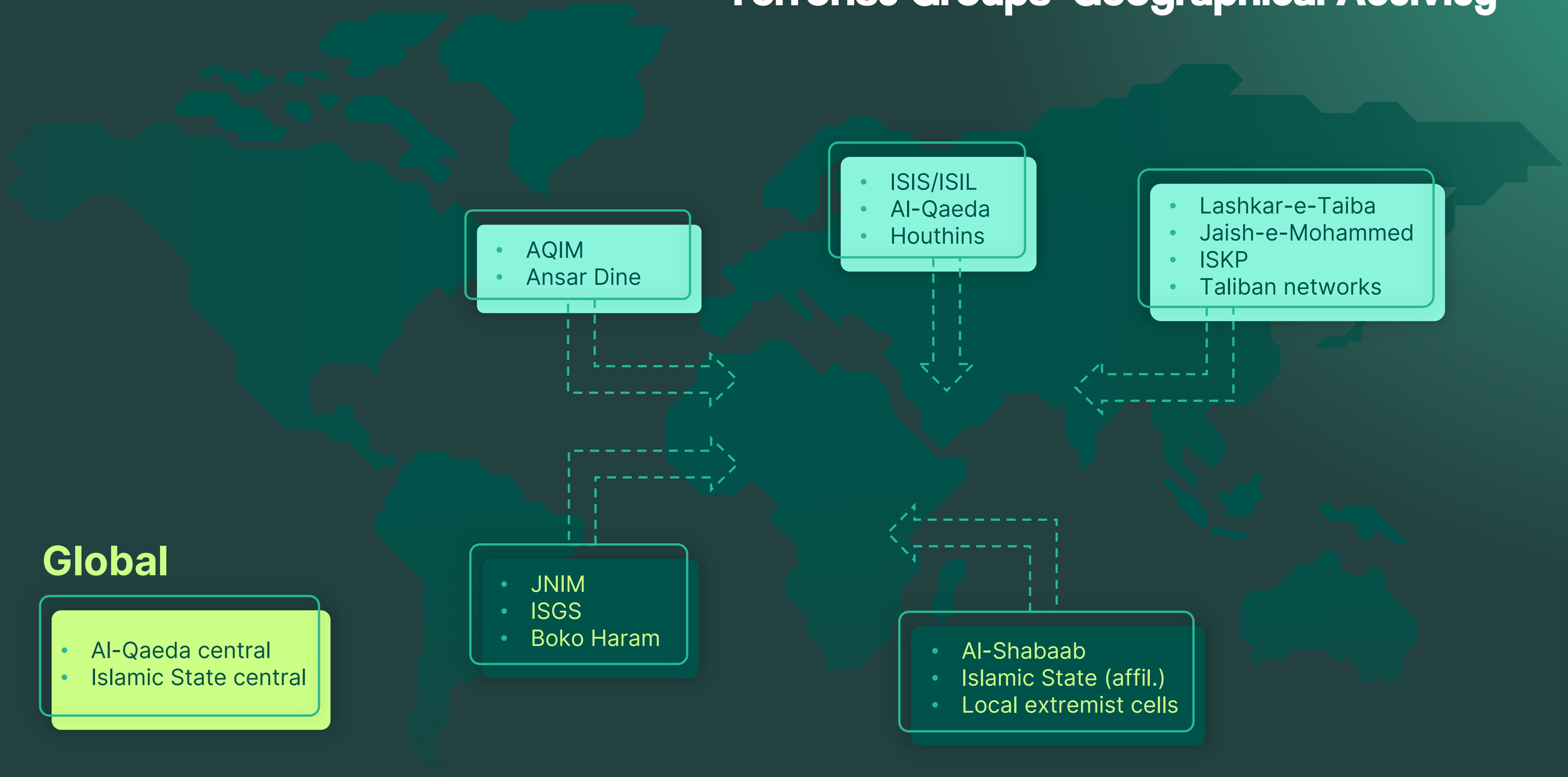
Sub-Saharan Africa and Central Asia noted as rising crypto risk hubs.

Fragile and conflict zones used to route illicit flows.

Example: Terrorist groups in Sahel receive support via crypto donations through third-party platforms.

Example: Shell NGOs in Central Asia acting as crypto channels for extremist fundraising.

Terrorist Groups' Geographical Activity



Global

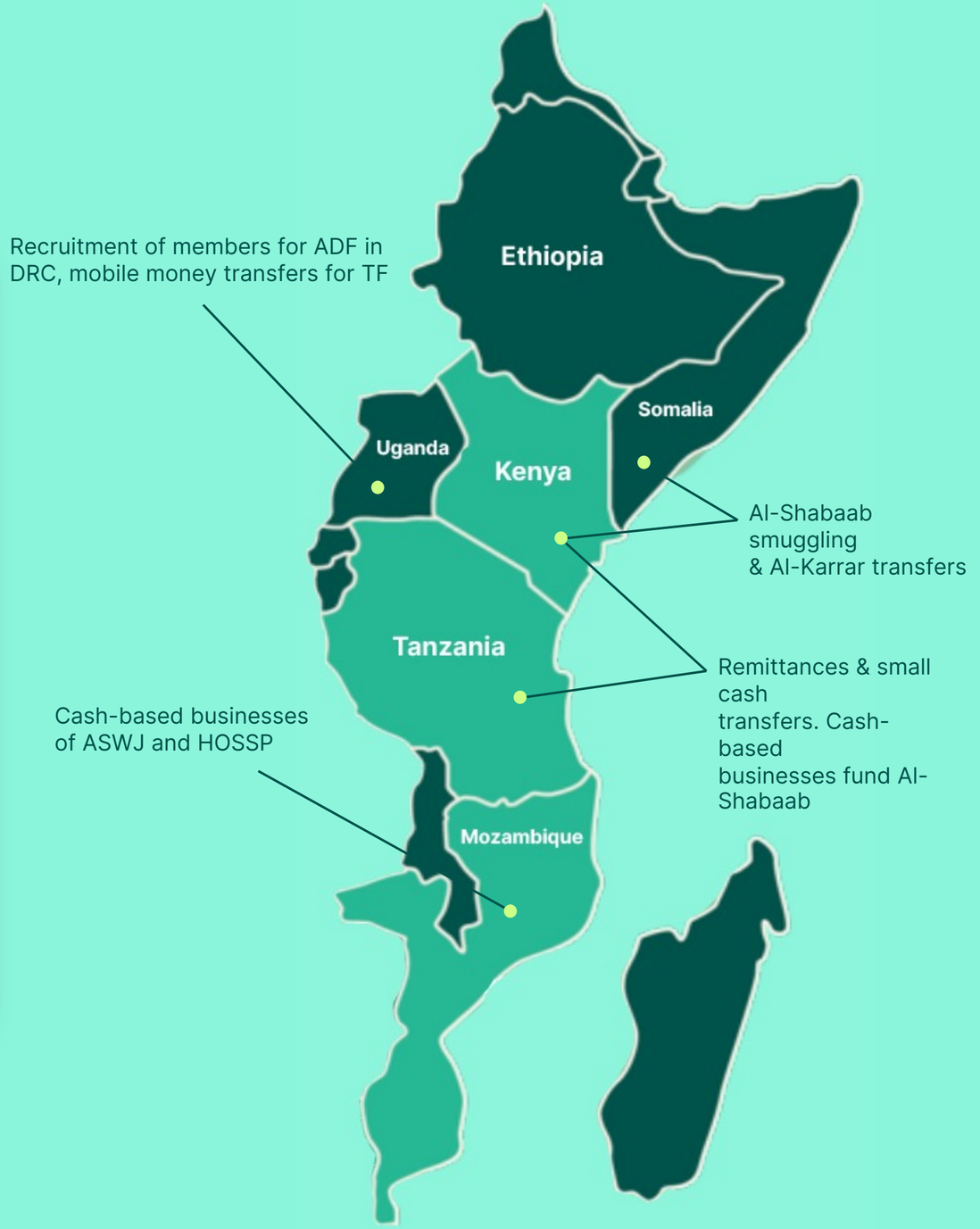
- Al-Qaeda central
- Islamic State central

East Africa's Evolving TF Threats

Regional Overview

- **Al-Shabab (Somalia/Kenya):** funding via extortion, local taxation, smuggling and cross-border trade.
- **Islamic State affiliates (Mozambique/DRC):** gold and natural-resource exploitation.
- **Kenya & Tanzania:** domestic cells relying on remittances and small cash transfers.
- **Uganda & Sudan:** transit and logistics hubs for regional TF networks.

According to local intelligence reports and FATF (2020-2025)



Certification Centre
By Crence

The Detection Mindset: From Reaction to Recognition

Recognise **Question** **Report**

Three steps to early detection:
1. Recognise typology patterns — don't treat alerts in isolation.
2. Ask contextual questions — *'Does this make commercial sense?'*
3. Report intelligently — STRs are intelligence, not punishment.

Certification Centre
By Crence

Certification Centre
By Crence

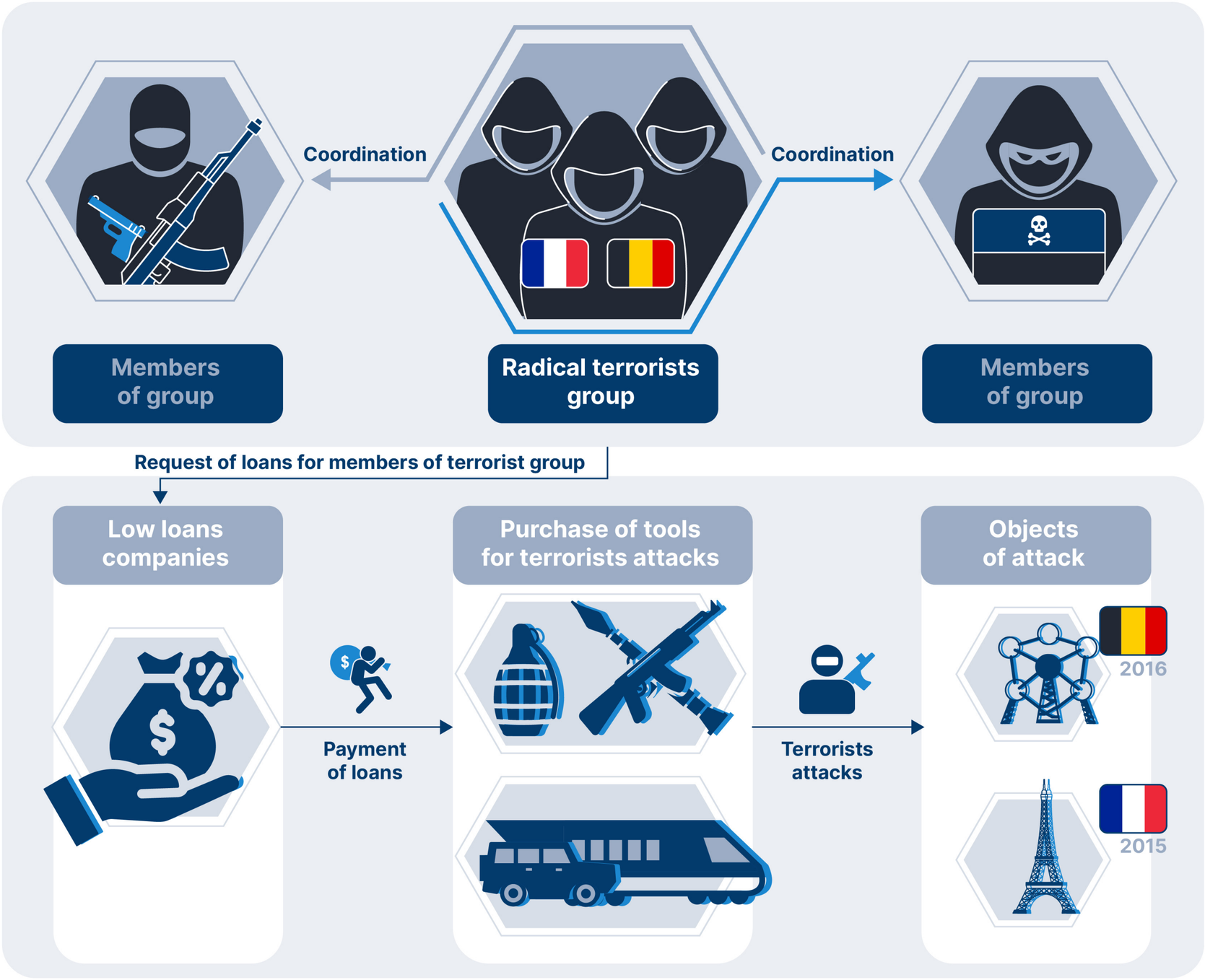
How the Financial Sector Can Interrupt the Flow of Criminal Funds – Real Cases & Tactics

Col. ret. Igoris Krzeckovskis
International Anti-Financial Crime Expert

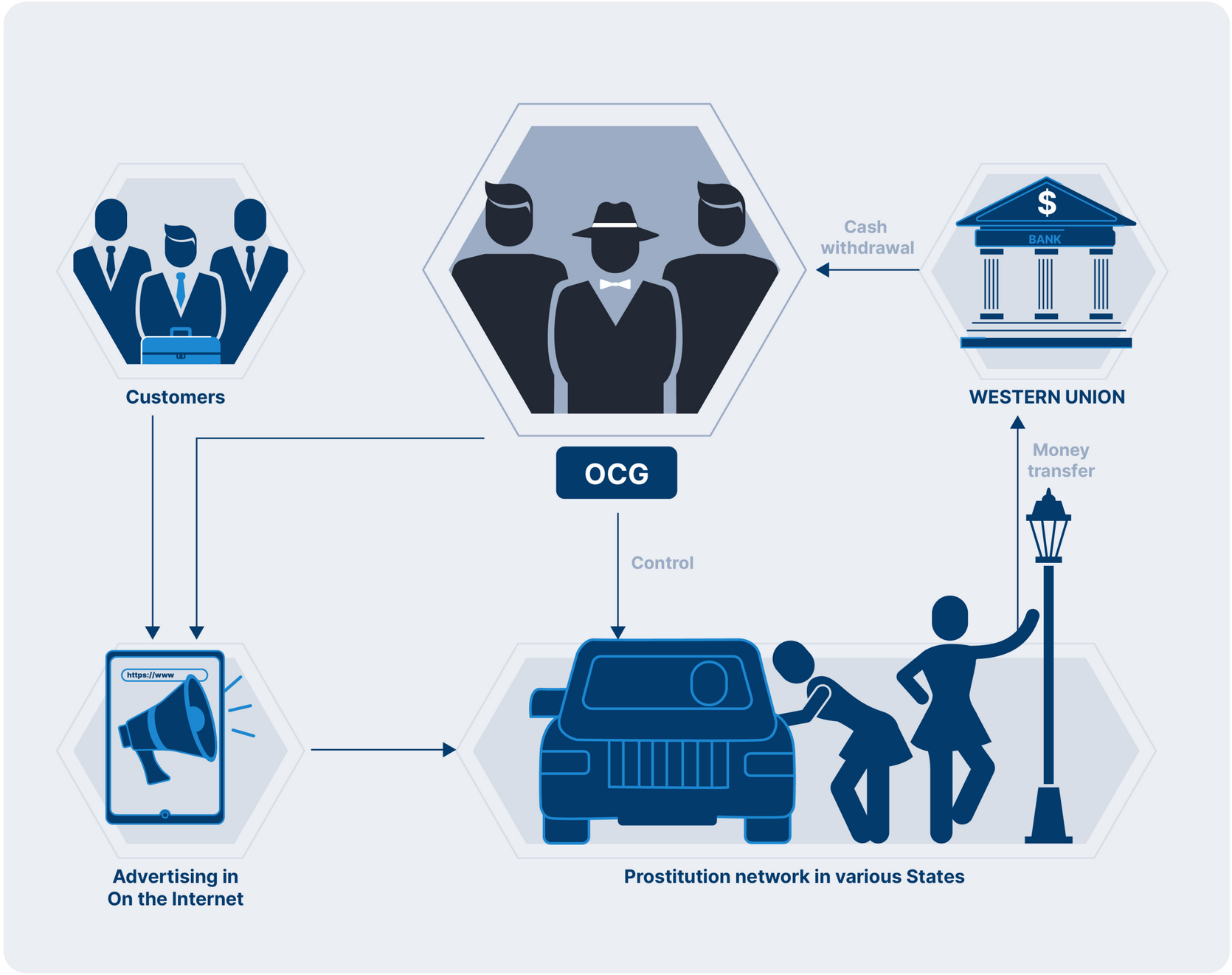
Certification Centre
By Crence

Frame the mindset — “Follow the money, interrupt the flow.”

Use of micro credit companies loans for terrorism financing

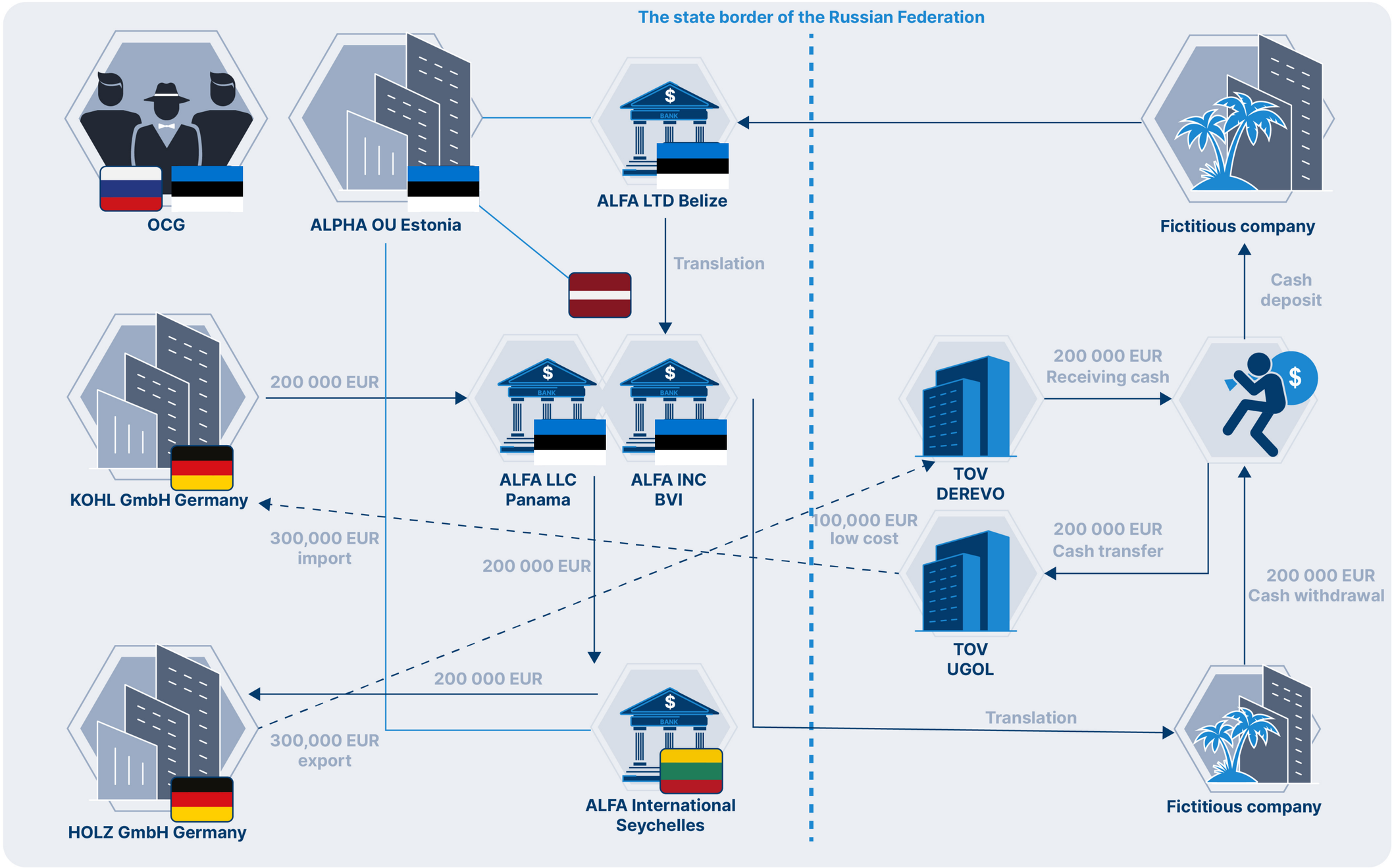


Prostitution and money laundering

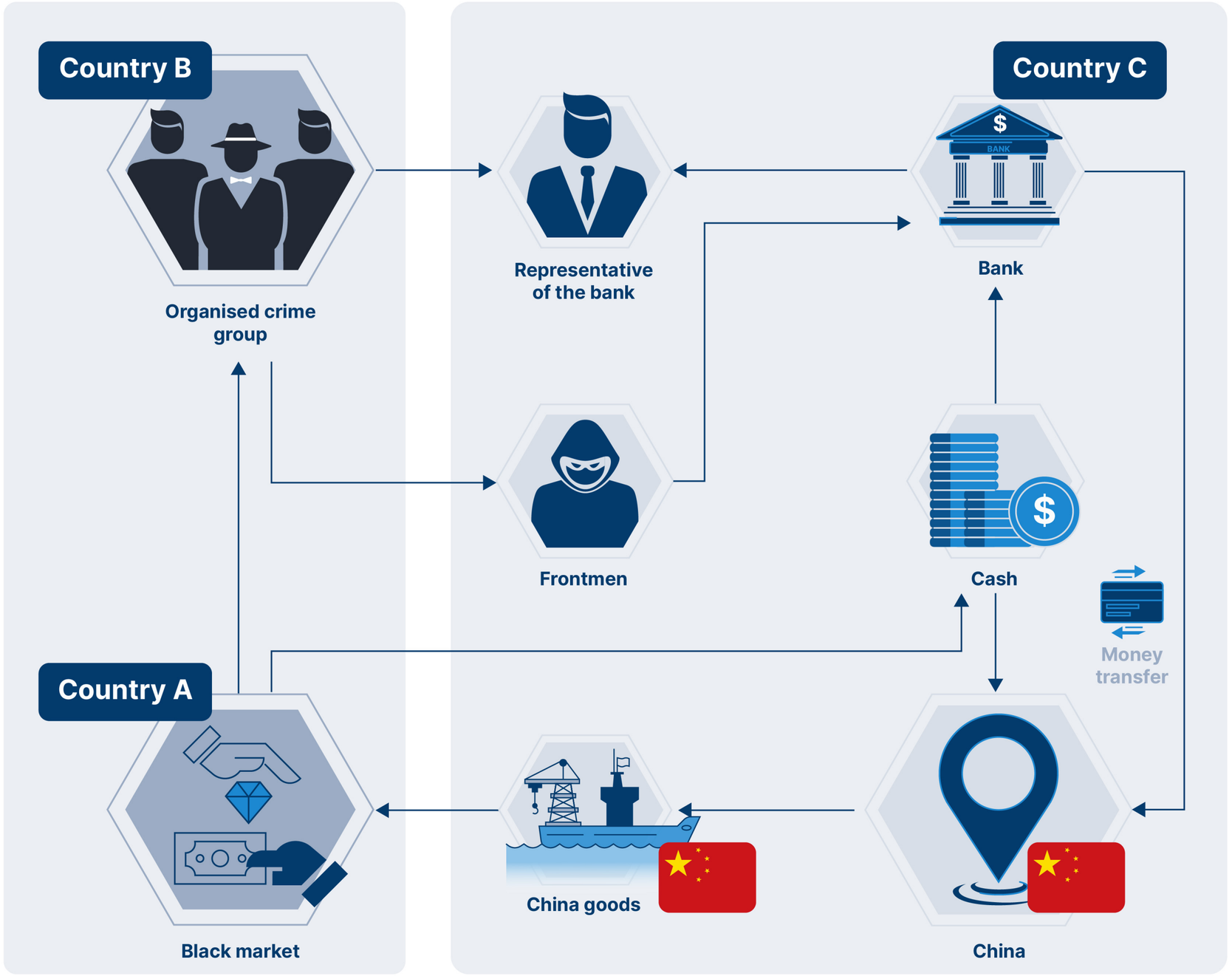


Illegal commercial activity and money laundering

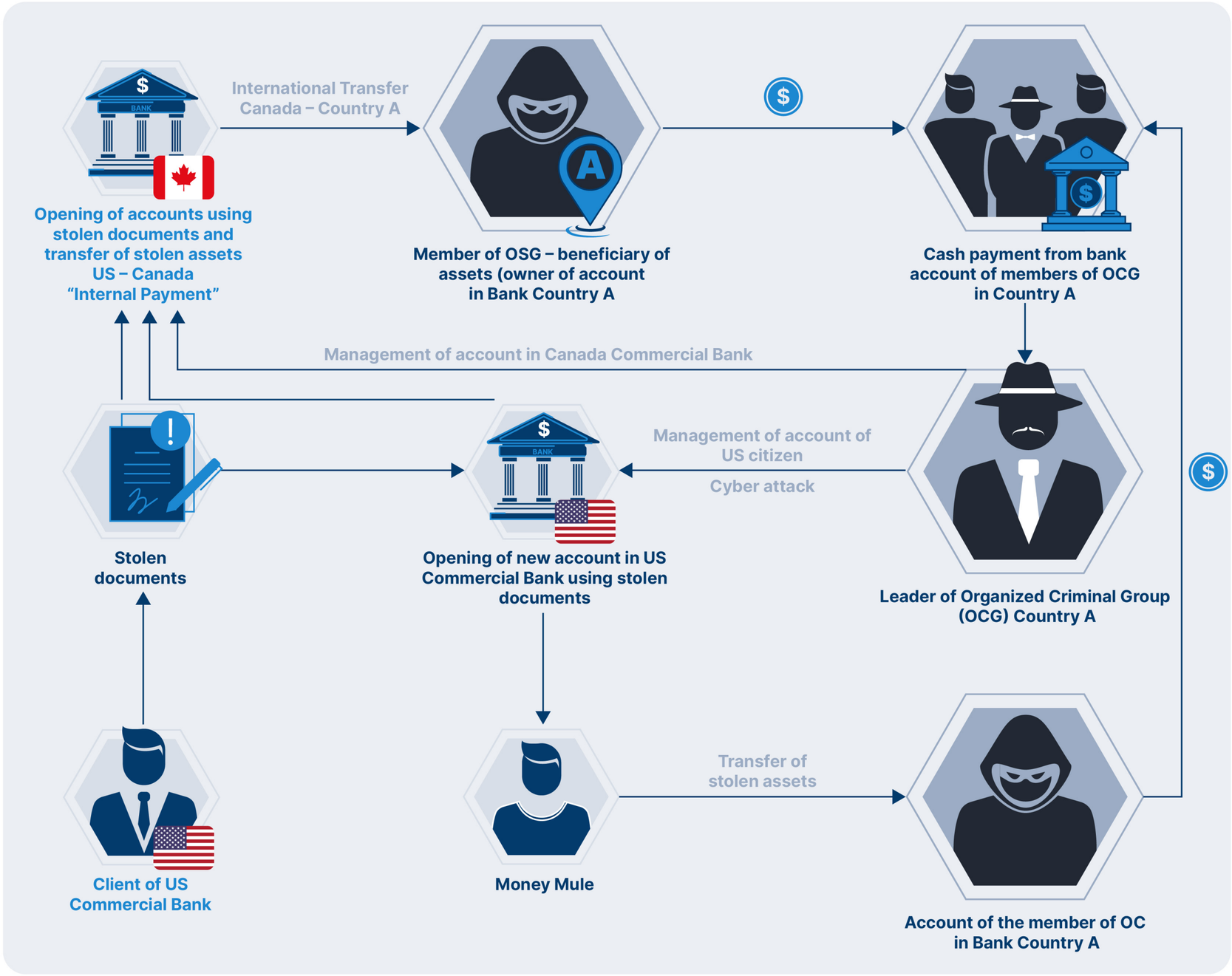
Organization of the settlement system in tax evasion and smuggling schemes



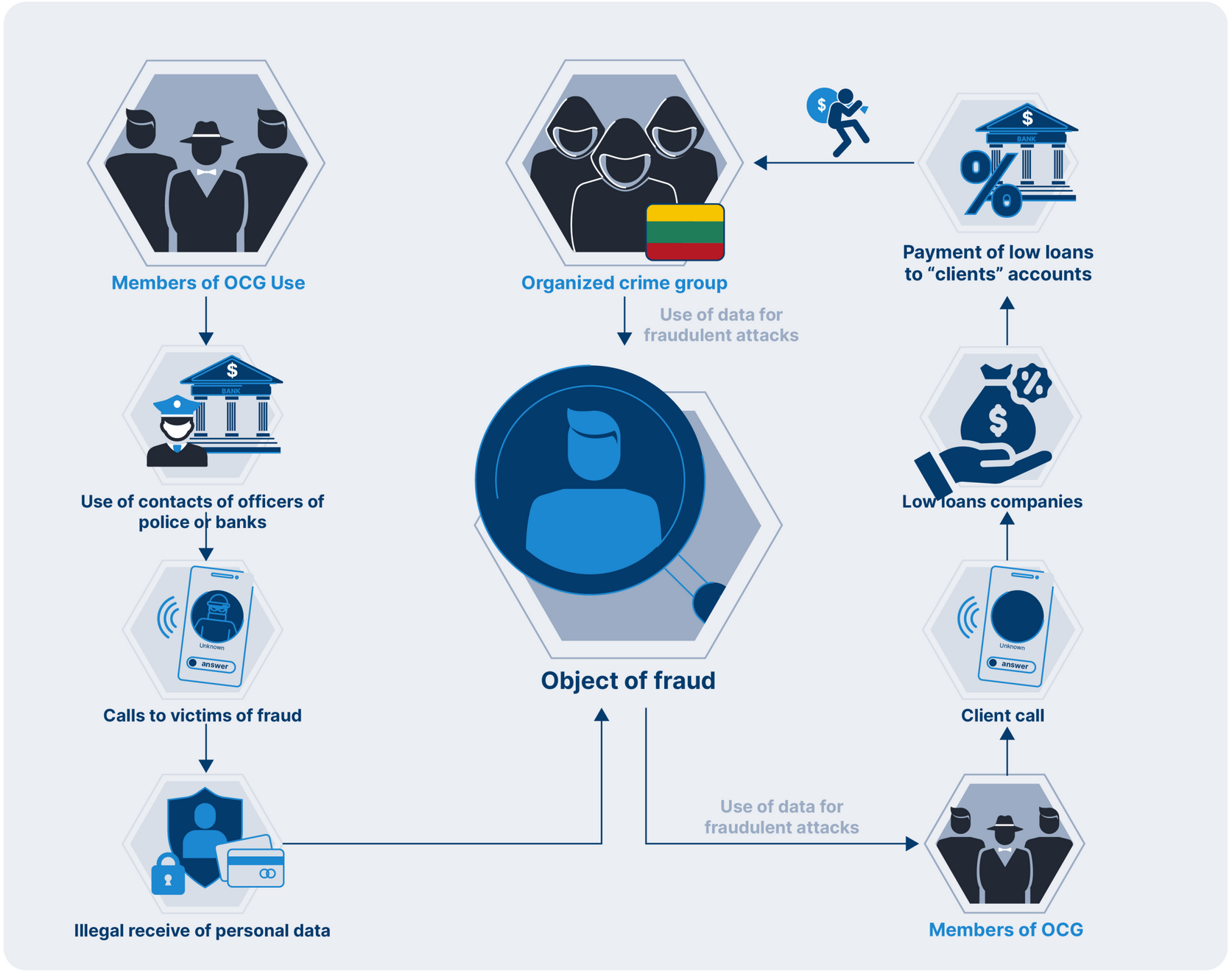
Cash smuggling, counterfeiting of banking documents, corruption and money laundering (trade-based ML)



Cyber Crime, Phishing, Fraud



Use of loans for fraudulent schemes



Certification Centre
By Crence

Frame the mindset — “Follow the money, interrupt the flow.”

Certification Centre By Crence

Avoiding Regulator Red Flags:

Best Practices in STRs and Reporting

Viktor Tkatsenko

Key Expert;
Head of AML, Citadele Bank

Certification Centre
By Crence

Chapter 1: The High Stakes of Suspicious Transaction Reporting

Certification Centre
By Crence

$55 Billion in AML Fines Since 2008

The financial industry has faced unprecedented regulatory enforcement, with over $55 billion in anti-money laundering penalties levied globally since 2008. These massive fines underscore regulator intolerance for STR failures and compliance gaps.

TD Bank's historic $3 billion fine in 2024 for systemic AML program deficiencies demonstrates the scale of risk institutions face when reporting obligations are not met.

Certification Centre
By Crence

What is an STR? The Frontline of Financial Crime Defense

Formal Documentation

A structured report filed when suspicious activity is detected in customer transactions or behavior

Critical Defense Tool

Key mechanism against money laundering, terrorist financing, fraud, and other financial crimes

Intelligence Sharing

Enables Financial Intelligence Units to identify patterns and coordinate law enforcement responses

Certification Centre
By Crence

STR vs SAR: Terminology Across Jurisdictions

STR (Suspicious Transaction Report)

- Preferred terminology in EU and by FATF
- Transaction-focused approach
- Emphasizes specific financial movements

SAR (Suspicious Activity Report)

- Primary term used in United States
- Broader activity-focused scope
- Encompasses patterns and behaviors

Despite terminology differences, the core obligation remains consistent: timely, accurate reporting of suspicious transactions that may indicate financial crime.

Who Must File STRs?

Financial Institutions

Banks, credit unions, payment service providers, investment firms and insurance providers

DNFBPs

Designated Non-Financial Businesses and Professions including lawyers, accountants, and casinos

Crypto Providers

Virtual asset service providers and digital currency exchanges

Real Estate Professionals

Agents and brokers handling high-value property transactions

Certification Centre
By Crence

Chapter 2: Recognizing Red Flags and Common Reporting Errors

Top Red Flags Triggering STRs

Unusual Transaction Patterns

Activity inconsistent with customer profile, business type, or historical behavior patterns

Structuring and Smurfing

Breaking large transactions into smaller amounts to avoid reporting thresholds or regulatory scrutiny

High-Risk Jurisdictions

Transactions involving countries with weak AML controls, sanctions, or known for financial crime

Complex Layering

Multiple transfers through various accounts or entities with no clear economic purpose

Structuring: The Classic Money Laundering Technique

What is Structuring?

Structuring involves breaking large sums into smaller deposits below reporting limits to evade detection. Criminals use multiple branches, third parties, or money mules to execute these transactions.

Key Indicators:

- Multiple deposits just under the KES 1,000,000 threshold
- Same-day transactions across different locations
- Activity inconsistent with customer profile
- Use of multiple individuals or accounts

Certification Centre
By Crence

Behavioral Red Flags

Customer Evasiveness

Reluctance or refusal to provide information about source of funds, beneficial ownership, or transaction purpose. Overly defensive responses to routine questions.

Sudden Behavioral Changes

Dramatic shifts in transaction behavior, volume, or patterns without reasonable explanation. Account dormancy followed by sudden high-value activity.

Lack of Economic Rationale

Complex transaction chains with multiple intermediaries serving no clear legitimate business purpose or creating unnecessary costs.

Common Reporting Errors That Raise Regulator Flags

Incomplete Information

Missing critical data fields on STR forms, including customer identifiers, transaction details, or supporting documentation

Vague Crime Classification

Failure to specify concrete crime sub-type or money laundering predicate offense, reducing report utility for investigators

Missed Deadlines

Filing beyond regulatory timelines, potentially allowing criminals to move funds or destroy evidence

Case Study: British Columbia Lottery Corporation Fine

C$1 Million Penalty

The British Columbia Lottery Corporation received a substantial fine for systematic failure to report suspicious transactions over an extended period.

Key Lessons:

- Timely reporting is non-negotiable
- Complete documentation prevents penalties
- Systemic failures attract maximum sanctions
- Reputational damage exceeds financial cost

Chapter 3: Reporting Timelines and Defensive Reporting

Certification Centre
By Crence

Certification Centre
By Crence

Reporting Timelines

Suspicion Identified

Transaction monitoring or staff observation triggers concern

1

Internal Review

Compliance team assesses and documents findings immediately

2

File STR

"As soon as practicable" - typically 24-72 hours depending on jurisdiction

3

FIU Receipt

Financial Intelligence Unit receives and processes for investigation

4

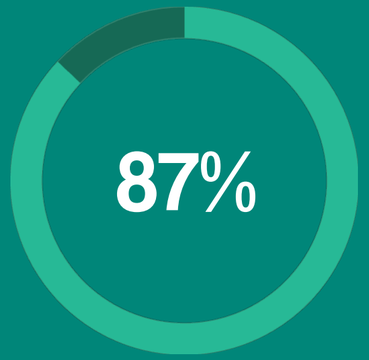
Delays increase risk of regulatory sanctions, evidence destruction, and fund dissipation.

Defensive Reporting: When in Doubt, Report Protected by Safe Harbor

Certification Centre
By Crence

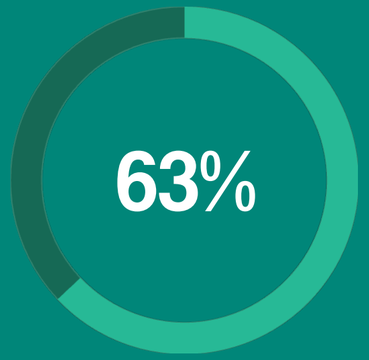
Reporting entities benefit from legal protections when filing STRs in good faith. Safe harbor provisions shield institutions from liability, even if suspicions prove unfounded.

Proactive reporting demonstrates commitment to compliance, reduces regulatory scrutiny, and protects against accusations of willful blindness.



Reduced Penalties

Institutions with strong reporting cultures



Better Outcomes

Cases resolved through defensive reporting

Best Practice: Avoid under-reporting to prevent penalties and reputational damage. The cost of over-reporting is minimal compared to the risk of missing suspicious activity.

Certification Centre
By Crence

Internal Reporting Procedures

Detection

Staff identifies suspicious activity through monitoring or customer interaction

Immediate Escalation

Front-line staff alerts designated compliance officer without delay

Review Process

Compliance team investigates, documents findings, and determines filing necessity

Decision & Filing

Senior officer approves STR submission with complete audit trail

Document all investigative steps meticulously to create defensible audit trail for regulatory examinations.

Chapter 4: Indicating Concrete Crime Sub-Types and ML Predicate Crimes

Certification Centre
By Crence

Why Specificity Matters in STRs

Certification Centre
By Crence

Vague or generic STRs provide limited value to Financial Intelligence Units and law enforcement. Specific crime classification enables:

- Efficient case prioritization and resource allocation
- Pattern recognition across multiple reports
- Targeted investigation strategies
- Cross-border intelligence sharing
- Enhanced prosecution success rates

EU guidelines explicitly require clear indication of predicate offenses such as tax evasion, fraud, drug trafficking, and corruption to maximize investigative effectiveness.

Common Predicate Crimes Under EU AML Framework

Certification Centre
By Crence

Tax Evasion & Fraud

Concealment of income, VAT fraud schemes, and offshore tax avoidance structures designed to evade legitimate tax obligations

Corruption & Bribery

Illicit payments to public officials, kickback schemes, and embezzlement of public or corporate funds

Human Trafficking

Modern slavery, forced labor exploitation, and organized criminal networks profiting from human suffering

Drug Trafficking

Narcotics distribution networks and proceeds from illegal drug trade requiring sophisticated laundering

Terrorist Financing

Funding of terrorist organizations, activities, or individual actors through legitimate or illicit channels

Cyber Fraud

Digital financial crimes including phishing, ransomware, business email compromise, and identity theft

Certification Centre
By Crence

How to Accurately Indicate Crime Sub-Type

Use Standardized Codes

Apply EBA-approved classification codes or descriptors that align with national FIU requirements and international standards

Provide Detailed Narrative

Include comprehensive explanation of transaction context, customer behavior, and specific basis for suspicion with supporting evidence

Link to Known Typologies

Reference established money laundering patterns, FATF typology reports, or intelligence from law enforcement where applicable

Include Supporting Data

Attach relevant documentation such as transaction records, customer communications, and due diligence findings

Certification Centre
By Crence

Chapter 5: EU Regulatory Landscape and Best Practices

AMLA (Anti-Money Laundering Authority) Role

Certification Centre
By Crence

Centralized EU Supervision

The Anti-Money Laundering Authority represents a watershed moment in EU financial crime prevention, centralizing supervision of high-risk financial institutions across member states.

Key Functions:

- Direct supervision of riskiest entities
- Harmonization of STR standards
- Cross-border enforcement coordination
- Development of EU-wide best practices

AMLA will become operational in 2024-2025, marking the most significant AML reform in EU history.

FATF Recommendations and EU Alignment

Global Standards

The Financial Action Task Force sets international standards for combating money laundering and terrorist financing, which form the foundation of EU regulations.

EU Implementation

EU directives and AMLA framework align closely with FATF's 40 Recommendations, ensuring consistent global approach.

1

Timely STR Filing

Immediate reporting obligations

2

Cross-Border Cooperation

Information sharing mechanisms

3

Beneficial Ownership

Transparency requirements

Certification Centre
By Crence

Certification Centre
By Crence

Leveraging Technology for STR Compliance

AI-Driven Transaction Monitoring

Advanced machine learning systems analyze patterns in real-time, generating sophisticated alerts that reduce false positives and identify complex schemes

Automated Data Enrichment

Systems automatically gather additional context from internal databases, public records, and third-party sources to enhance report quality

CDD & KYC Integration

Seamless integration with customer due diligence and know-your-customer data provides comprehensive view of customer risk profile

Staff Training and Awareness

Certification Centre
By Crence

Building a Culture of Vigilance

Effective STR programs require more than systems—they demand skilled, alert staff who understand their critical role in financial crime prevention.

- **Regular Training Updates**

  Continuous education on emerging typologies, new red flags, and evolving criminal methodologies

- **Scenario-Based Exercises**

  Practical simulations improve detection skills and reporting confidence through realistic case studies

- **Compliance Culture**

  Leadership commitment that encourages vigilance, transparency, and proactive reporting without fear

Certification Centre
By Crence

Chapter 6: The Path to Compliance Excellence

Certification Centre
By Crence

Building a Robust STR Program

Clear Policies & Procedures

Comprehensive written policies aligned with EU AMLA, EBA guidelines, and national requirements with regular review cycles

Strong Governance

Defined roles, accountability framework, and senior management oversight with board-level reporting

Technology Infrastructure

Sophisticated monitoring systems integrated with customer databases and risk assessment tools

Continuous Improvement

Regular audits, regulator feedback incorporation, and adaptation to emerging threats and typologies

Real-World Impact: Protecting Your Institution and Society

Certification Centre
By Crence

Beyond Compliance

Effective STR programs deliver value far beyond regulatory checkbox exercises. They represent your institution's contribution to global security and financial integrity.

$2T

Annual ML Volume

Estimated globally laundered funds

78%

Network Disruption

Criminal operations impacted by STRs

Key Benefits:

- Disrupt criminal and terrorist networks
- Avoid costly fines and sanctions
- Protect institutional reputation
- Contribute to financial system integrity
- Safeguard vulnerable populations

Conclusion: Stay Ahead of Regulator Red Flags

Timely & Accurate STRs

Prioritize complete, well-documented reports filed within regulatory deadlines with specific crime classifications

Defensive Reporting Culture

Embrace "when in doubt, report" philosophy and provide continuous staff training on evolving threats

Regulatory Alignment

Maintain compliance with EU AMLA, EBA, and FATF best practices through ongoing program refinement

---

Your vigilance is the frontline defense against financial crime

By implementing these best practices, your institution not only avoids regulatory sanctions but becomes a crucial partner in protecting the global financial system and society at large.

Certification Centre
By Crence

Mastering CDD and BO: Getting Risk-Rated KYC Right

Risk-Based Approach, EU vs African Registers & Verification Challenges

Certification Centre

By Crence

Closed Door Regulators' Roundtable:

AML/CTF Risk-Based Supervision

Empowering Reuglators and Financial Institutions Globally

Certification Centre
By Crence

Chapter 1: The Foundations of Risk-Based KYC

Understanding Customer Due Diligence and Beneficial Ownership in the context of modern AML/CFT compliance frameworks

Certification Centre
By Crence

What is Customer Due Diligence (CDD)?

Customer Due Diligence is a comprehensive process designed to verify customer identity and assess their money laundering and terrorist financing risk profile. It forms the backbone of anti-money laundering and counter-terrorist financing frameworks worldwide.

CDD is mandated by the Financial Action Task Force (FATF) recommendations and implemented through EU directives, requiring financial institutions to know their customers before establishing business relationships.

Certification Centre
By Crence

Beneficial Ownership (BO): The Hidden Layer

Ultimate Ownership

Identifying the natural persons who ultimately own or control legal entities, typically those holding 25% or more ownership stake

Preventing Misuse

Critical to prevent the misuse of corporate structures, shell companies, and complex ownership chains for illicit finance and tax evasion

Transparency Chain

Requires tracing through layers of ownership to reveal the real individuals behind corporate veils and nominee arrangements

Certification Centre
By Crence

Why Risk-Based Approach (RBA)?

Tailored Due Diligence

The risk-based approach tailors the intensity and depth of due diligence measures to match each customer's specific risk profile, ensuring resources focus where risks are highest.

Financial Inclusion Balance

Balances robust regulatory compliance with financial inclusion objectives, ensuring legitimate customers aren't excluded due to overly rigid requirements.

Operational Efficiency

Avoids "one-size-fits-all" inefficiencies that waste resources on low-risk customers while potentially missing high-risk indicators in complex cases.

The Risk Spectrum in Action

Low Risk

Simplified Due Diligence - basic verification, minimal documentation, expedited onboarding

Medium Risk

Standard CDD - comprehensive identity verification, purpose of relationship, ongoing monitoring

High Risk

Enhanced Due Diligence - intensive scrutiny, senior approval, continuous monitoring, source of wealth verification

AML Certification Centre By Crence

EU Regulatory Landscape: EBA Guidelines & AML Directive

01

EBA Guidelines 2021/02

Amended in 2023, these guidelines set detailed ML/TF risk factors for credit and financial institutions across the EU

02

5th AML Directive

Directive (EU) 2015/849 mandates comprehensive risk-based CDD and establishment of beneficial ownership registers

03

GDPR Integration

General Data Protection Regulation significantly impacts data handling, privacy rights, and retention in KYC processes

AML Certification Centre
By Crence

Certification Centre
By Crence

EU BO Registers: Transparency & Verification

2019: Register Launch

Centralized public registers of beneficial owners established across EU member states, marking a new era of corporate transparency

1

2

Verification Challenges

Ongoing issues with data accuracy, completeness, cross-border consistency, and verification of self-reported information

Supervisory Evolution

3

Continuous efforts by national authorities to improve register reliability through enhanced verification mechanisms and sanctions for non-compliance

Despite progress, the EU faces significant challenges in ensuring data quality and preventing the use of nominee directors and complex ownership structures to obscure true beneficial owners.

African KYC Registers: Diversity & Innovation

Varied Maturity

- Nigeria's Bank Verification Number (BVN) system
- South Africa's advanced digital ID infrastructure
- Kenya's mobile-based identity solutions
- Wide gaps between countries

Key Challenges

- Incomplete population coverage
- Limited interoperability across borders
- Data quality and verification issues
- Infrastructure constraints

Innovations

- Mobile-first e-KYC solutions
- Biometric verification systems
- Tiered due diligence models
- Agent-based verification networks

Certification Centre
By Crence

Global KYC Infrastructure Maturity

27

EU Member States

With harmonized BO registers and interoperability frameworks in place

15%

African Countries

Have implemented comprehensive centralized beneficial ownership registers

60%

Digital Gap

Of African population still lacks formal digital identity credentials

AML Certification Centre By Crence

Chapter 2: Risk Levels in KYC

Defining and Applying Risk Ratings in Customer Due Diligence

Certification Centre
By Crence

KYC Risk Levels Explained

Low Risk

Simplified Due Diligence (SDD) is permitted for customers presenting minimal ML/TF risk

- Reduced verification requirements
- Streamlined documentation
- Faster onboarding processes

Medium Risk

Standard CDD measures apply to the majority of customers

- Comprehensive identity verification
- Purpose of relationship assessment
- Regular monitoring protocols

High Risk

Enhanced Due Diligence (EDD) is mandatory for elevated risk profiles

- Intensive background checks
- Senior management approval
- Continuous transaction monitoring

Certification Centre
By Crence

Risk Factors to Consider

EBA Guidelines Highlights

Customer Type

Legal form, ownership structure, business activities, and reputation of the customer entity or individual

Geography

Customer residence, business location, and countries involved in transactions - considering sanctions, corruption levels, and AML frameworks

Product/Service Risk

Complexity, anonymity potential, and value of products or services offered to or used by the customer

Transaction Patterns

Complexity, volume, size, and frequency of transactions, including deviation from expected behavior

PEPs & Adverse Media

Politically Exposed Persons status, family connections, and presence of negative news or sanctions screening hits

African Context: Risk Factors & Practical Challenges

Certification Centre
By Crence

Unique Risk Factors

Informal Economy

Large cash-based transactions and informal business activities that are difficult to verify and monitor

Documentation Gaps

Limited availability of official identity documents for significant portions of the population, especially in rural areas

Cross-Border Complexity

High volume of remittances and correspondent banking relationships requiring enhanced monitoring

The predominance of cash-based transactions and informal economic activities in many African markets presents unique challenges for traditional risk assessment frameworks designed for formal banking systems.

Case Study: South Africa's Risk-Based KYC Implementation

Tiered CDD Adoption

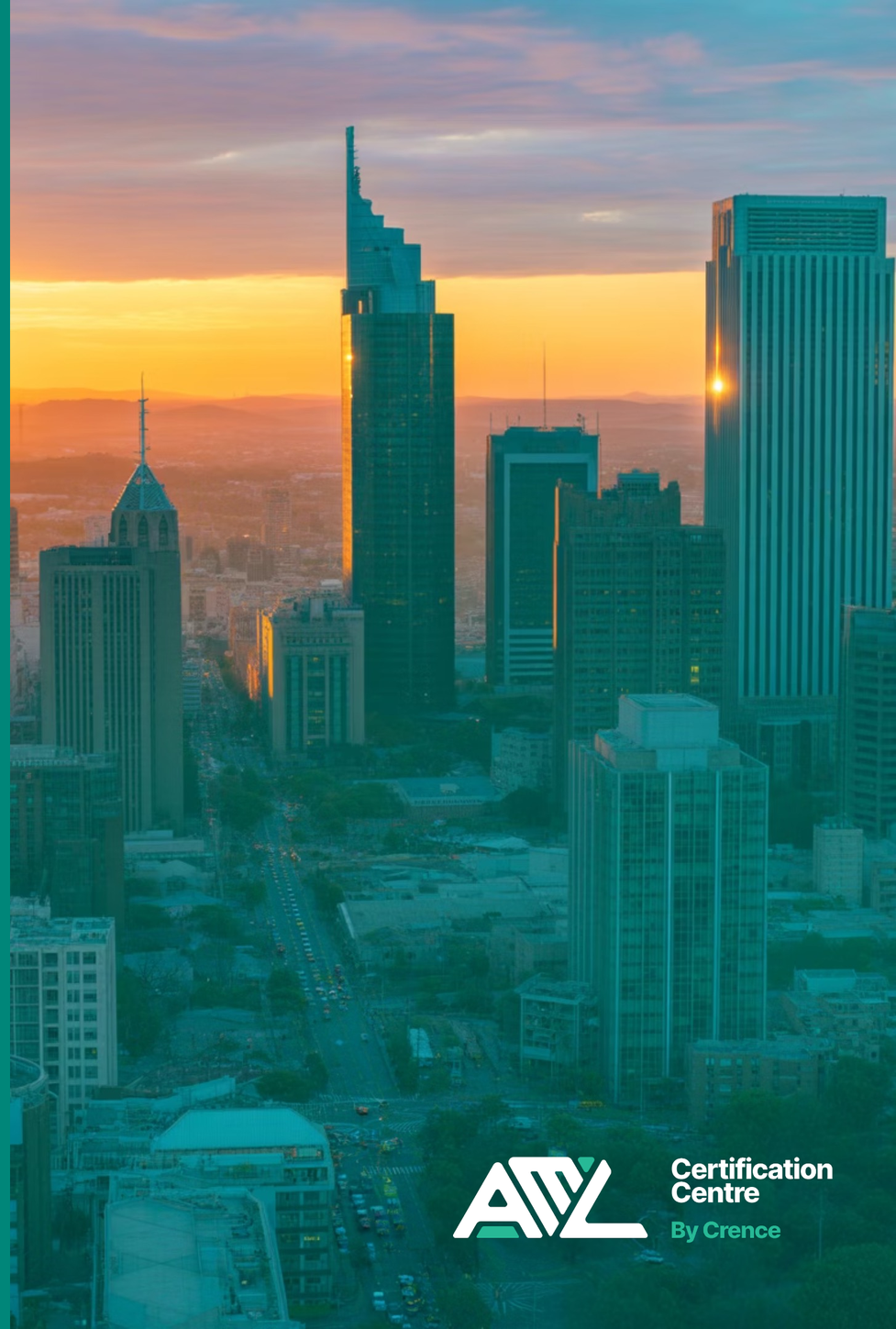
Implementation of differentiated due diligence requirements to promote financial inclusion while maintaining compliance standards

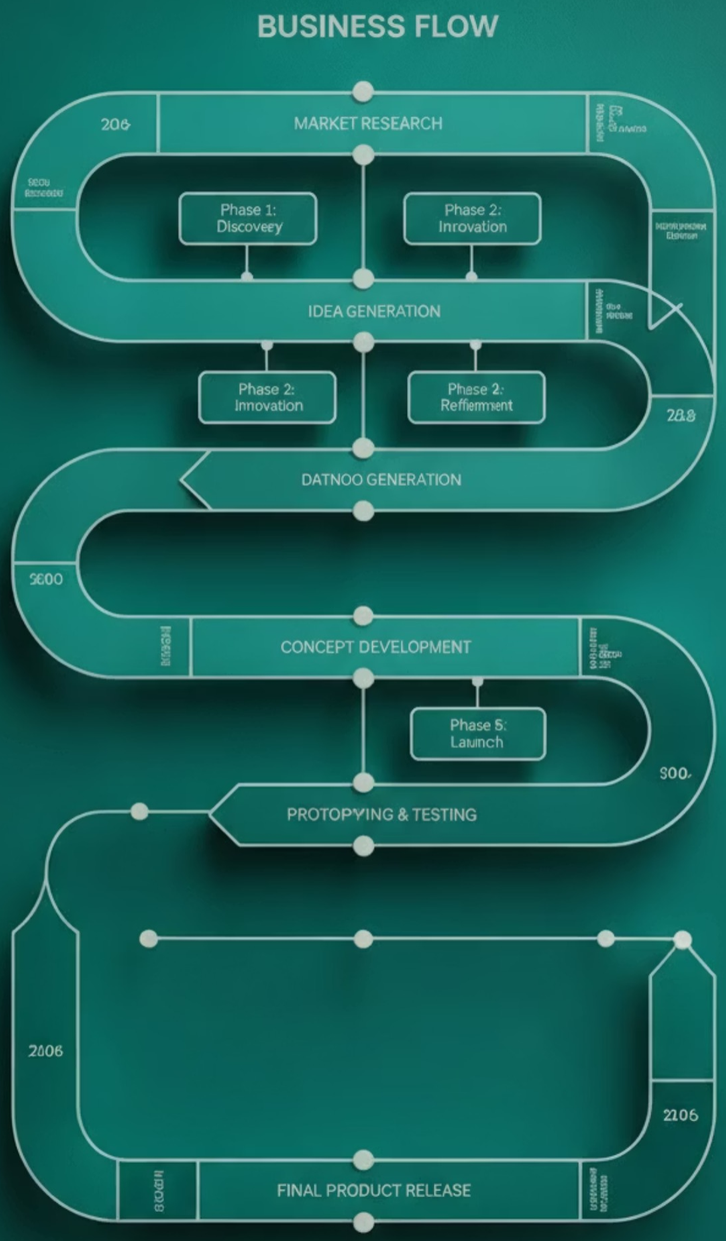
Biometric Integration

Deployment of biometric verification and digital identity systems to mitigate verification gaps and reduce fraud

Persistent Challenges

High implementation costs, data sharing limitations between institutions, and need for greater regulatory harmonization across SADC region





Certification Centre
By Crence

Risk Assessment Process Flow

1

Customer Onboarding

Initial risk assessment based on customer type, geography, expected activity, and product selection

2

Information Gathering

Collection of identification documents, beneficial ownership data, and purpose of relationship information

3

Risk Rating Assignment

Application of risk scoring methodology to assign appropriate risk level and determine CDD measures

4

Ongoing Monitoring

Continuous transaction monitoring, periodic review, and dynamic risk reassessment based on behavior and external factors

Chapter 3: BO Registers and Verification Challenges

Navigating Complexity in Beneficial Ownership Transparency

Certification Centre
By Crence

EU BO Register Verification Challenges

Certification Centre
By Crence

1

Data Accuracy Issues

Self-reported information often lacks independent verification, leading to incomplete or inaccurate beneficial ownership data in registers

2

Entity Complexity

Complex corporate structures with multiple layers, nominee shareholders, and trusts obscure true beneficial ownership chains

3

Cross-Border Limitations

Limited data sharing mechanisms between EU member states and non-EU jurisdictions hinder complete ownership verification

4

Update Delays

Time lag between ownership changes and register updates creates windows where information becomes outdated or misleading

African BO Verification Challenges

Certification Centre
By Crence

Absence of Central Registers

Many African countries lack centralized or publicly accessible beneficial ownership registers, forcing reliance on company filings and manual searches

Fragmented Frameworks

Regulatory frameworks vary significantly across regions like ECOWAS, SADC, and EAC, with limited harmonization efforts

Manual Processes

Heavy reliance on paper-based records and manual verification processes increases processing time, costs, and error rates

Certification Centre
By Crence

Technology as a Game-Changer

Blockchain & DLT

Distributed ledger technology creates immutable, transparent records of beneficial ownership that can be accessed by authorized parties while maintaining data integrity

Biometric Verification

Integration of biometric systems and digital identity platforms enables secure, fast, and reliable identity verification across channels

RegTech Solutions

Advanced RegTech platforms provide real-time risk scoring, automated monitoring, and intelligent alert systems for suspicious activities

Certification Centre
By Crence

Comparative Insight: EU vs African Verification Approaches

European Union

Regulatory Mandates

Strong legal frameworks with mandatory BO registers and harmonized standards

Digital Evolution

Evolving digital registers with improving interoperability and API access

Persistent Issues

Data accuracy, nominee arrangements, and cross-border verification gaps remain

Africa

Innovation Drive

Innovation driven by financial inclusion needs and mobile technology adoption

Infrastructure Gaps

Limited infrastructure and fragmented regulatory landscape across jurisdictions

Interoperability

Both regions face challenges in data interoperability and verification reliability

Chapter 4: Overcoming KYC and BO Verification Challenges

Practical Solutions for Enhanced Compliance and Efficiency

Certification Centre
By Crence

Certification Centre
By Crence

Best Practices for Effective Risk-Rated KYC

01

Implement Tiered Due Diligence

Develop and deploy differentiated CDD procedures that align precisely with assigned risk levels, ensuring appropriate resource allocation

02

Leverage Third-Party Data

Utilize reputable data providers, sanctions watchlists, PEP databases, and adverse media screening tools to enhance verification

03

Continuous Monitoring

Establish robust ongoing monitoring programs with dynamic risk reassessment based on transaction behavior and external risk factors

04

Quality Assurance

Regular audits of KYC processes, documentation quality, and risk rating accuracy to ensure compliance and effectiveness

Addressing Data Privacy and Compliance

EU GDPR Compliance

Key Requirements:

- Lawful basis for processing personal data in KYC
- Data minimization and purpose limitation principles
- Customer rights to access, rectification, and erasure
- Strict data retention and deletion schedules
- Enhanced security measures and breach notification

African Data Protection

Evolving Landscape:

- Growing number of data protection laws (e.g., South Africa's POPIA)
- Significant gaps in enforcement capabilities
- Varied maturity levels across jurisdictions
- Need for harmonization with international standards
- Balance between transparency and privacy rights

Successfully navigating data protection requirements while maintaining effective KYC processes requires careful balancing of transparency obligations with individual privacy rights.

Certification Centre
By Crence

Enhancing BO Transparency and Verification

Strengthen Legal Frameworks

Develop comprehensive legal requirements for beneficial ownership disclosure with meaningful penalties for non-compliance and false reporting

Regional Cooperation

Encourage cross-border data sharing agreements, mutual legal assistance treaties, and harmonized standards within economic communities

Public-Private Partnerships

Foster collaboration between government agencies and private sector to improve data accuracy, verification processes, and technology adoption

Verification Mechanisms

Implement independent verification processes beyond self-reporting, including notary requirements and documentary evidence standards

Innovations Driving the Future of KYC & BO

AI & Machine Learning

Advanced algorithms for pattern detection, anomaly identification, and intelligent risk scoring that adapt and learn from transaction data

Mobile-First e-KYC

Smartphone-based verification solutions expanding financial access in Africa through selfie verification, document scanning, and biometric capture

Blockchain Records

Distributed ledger technology creating tamper-proof, transparent beneficial ownership records with controlled access and audit trails

API Integration

Real-time data sharing through secure APIs connecting financial institutions, regulators, and data providers for instant verification

Certification Centre
By Crence

Digital Transformation in KYC

1

Paper Era

Manual forms, physical document copies, in-person verification, filing cabinets

2

Digital Scanning

Document digitization, electronic storage, basic database systems

3

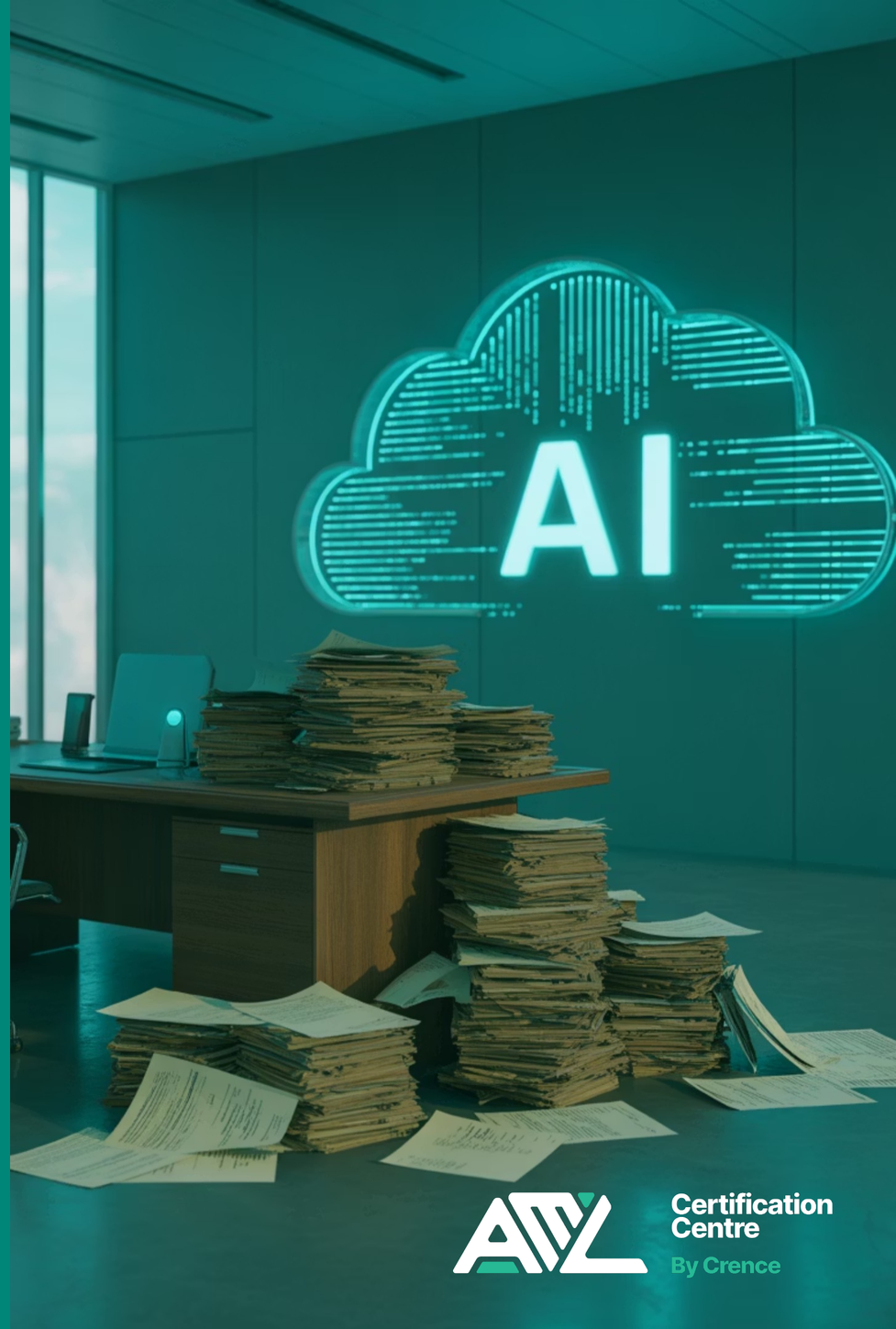
Automated Processing

OCR technology, automated data extraction, electronic verification

4

AI-Powered Platforms

Machine learning, real-time risk assessment, predictive analytics, blockchain integration



Certification Centre
By Crence

Certification Centre
By Crence

Chapter 5: Strategic Recommendations & The Road Ahead

Building a Framework for Sustainable Compliance Excellence

Key Recommendations

Certification Centre
By Crence

1

Harmonize Regulations

Promote harmonization of KYC and beneficial ownership regulations at regional (EU, AU, ECOWAS, SADC) and international levels to reduce compliance complexity

2

Invest in Infrastructure

Develop interoperable digital identity systems and verification infrastructure that work seamlessly across borders and institutions

3

Build Capacity

Foster comprehensive capacity building programs for regulators, compliance officers, and financial institutions through training and knowledge sharing

4

Embrace Technology Responsibly

Adopt innovative technology solutions while maintaining robust safeguards for privacy protection and financial inclusion principles

5

Collaborate Across Sectors

Encourage public-private partnerships and international cooperation to share best practices, data, and technology solutions

Certification Centre
By Crence

Conclusion: Mastering Risk-Rated KYC for a Safer, Inclusive Financial Future

Foundational Pillars

Effective CDD and beneficial ownership verification are essential pillars of successful AML/CFT frameworks globally

Balanced Approach

Risk-based approaches enable the critical balance between robust compliance requirements and financial inclusion objectives

Collective Action

Collaboration across borders and innovation in technology are essential to overcome persistent verification challenges

Let's build trust and transparency across borders together - creating financial systems that are both secure against illicit finance and accessible to legitimate customers worldwide.

Q&A Session

Certification Centre
By Crence

Thank you!

Certification Centre
By Crence