data | cros 3

Co-funded by the European Union

DATACROS III

Developing an Ethical AI-driven Tool-box for Boosting Cross-border Financial Investigations on Organised Crime Networks

INTEGRITY & DUE DILIGENCE

Michael Lo Giudice
Michaelvictor.logiudice@unicatt.it

BACKGROUND & CONTEXT

BACKGROUND & CONTEXT

Today's organized & financial crime:

- exploits the **corporate, banking, and real estate sectors**
- **misuses legal business structures**
- **co-mingles illicit proceeds with public money** (subsidies and public procurement)
- employs cash, digital, and **virtual currencies**
- adopts **cross-border schemes**
- builds complex corporate structures
- **capitalizing on AI** for carrying out next-gen financial crimes (e.g., **cloned voices & deep fakes** for fraud)

NEEDS TO BE ADDRESSED

Keeping pace:

- **data on a wider range of financial and asset domains**
- **advancing algorithm and risk assessment modules**
- assessing **the use of AI-driven tools**
- **exchange of information and best practices**
- dedicated **training on monitoring skills**

NEEDS TO BE ADDRESSED

Keeping pace:

- **data on a wider range of financial and asset domains**
- **advancing algorithm and risk assessment modules**
- assessing **the use of AI-driven tools**
- **exchange of information and best practices**
- dedicated **training on monitoring skills**

Addressed by DATACROS III Project

OUR TEAM

DCIII – CONSORTIUM

COORDINATOR

TRANSCRIME
Joint Research Centre on Innovation and Crime

INVESTIGATIVE JOURNALISTS

context
OCCRP
RPI MEDIA

PUBLIC/PRIVATE SECTOR

RESEARCH ACTION
EUROPEAN BUSINESS REGISTRY ASSOCIATION
GLEIF
Enabling global identity
Protecting digital trust

LEAs, AROs, & FIUs

ANABI
SCO
Financial Intelligence Unit

TECH/DATA PARTNERS

Regnology
CERTH
crime&tech
UNIVERSITÀ CATTOLICA del Sacro Cuore
Crystal
Government Transparency Institute

COMPETITION & CORRUPTION

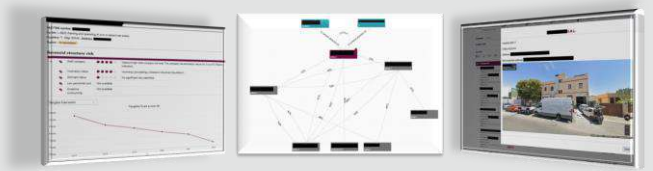
KONKURRANSE TILSYNET
ANAC
Autorité de la concurrence
ÚOHS
NTA
NATIONAL TRANSPARENCY AUTHORITY

OUR ACTIVITIES

DATACROS III ACTIVITIES

RESEARCH

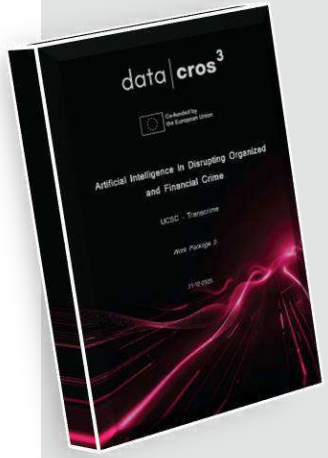
DEVELOPING TOOLS



TRAINING SESSIONS

THE DATACROS III MISSION

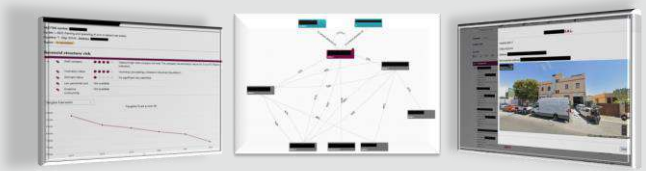
RESEARCH



RESEARCH PAPERS, WHITE PAPERS & POLICY REPORTS

UNDERSTANDING RISK ON NEW DIMENSIONS

DEVELOPING TOOLS



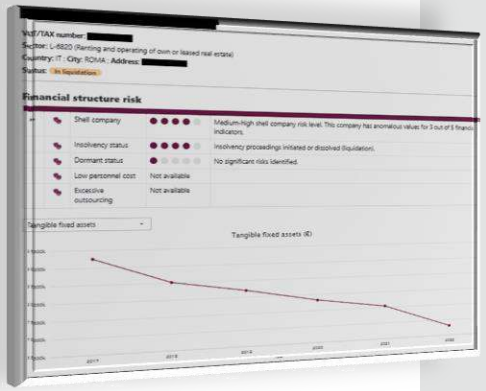
TRAINING SESSIONS

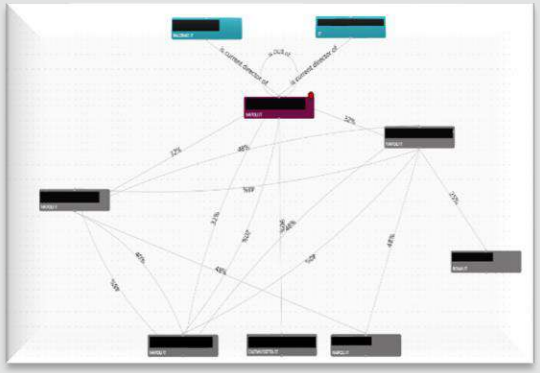
THE DATACROS III MISSION

RESEARCH

DEVELOPING TOOLS

DATACROS III PLATFORM



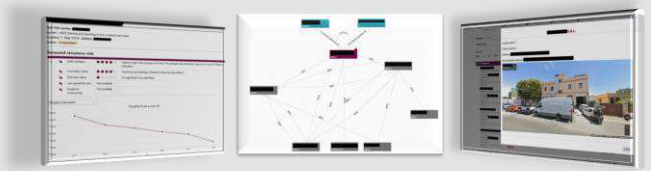


TRAINING SESSIONS

THE DATACROS III MISSION

RESEARCH

DEVELOPING TOOLS



TRAINING SESSIONS

Today's Training

INTEGRITY & DUE DILIGENCE

- Focus on AML-obliged Entities
- Comprehending and reacting to organized and financial crime

data | cros^3

www.datacros3.com

AGENDA – First Session

09.45	**Introduction** Michael Lo Giudice (Università Cattolica del Sacro Cuore - Transcrime)
10.00	**Session 1: The Landscape of Organised Crime in the Corporate Sector** Pawel Martyniuk (Regnology)
10.45	**Session 2: Early-Warning Indicators in Customer Due Diligence (CDD)** Lukasz Wojciechowski (Regnology)
11.30	**Coffee Break**

data | cros^3 TRANSCRIME UNIVERSITÀ CATTOLICA del Sacro Cuore Regnology

AGENDA – Second Session

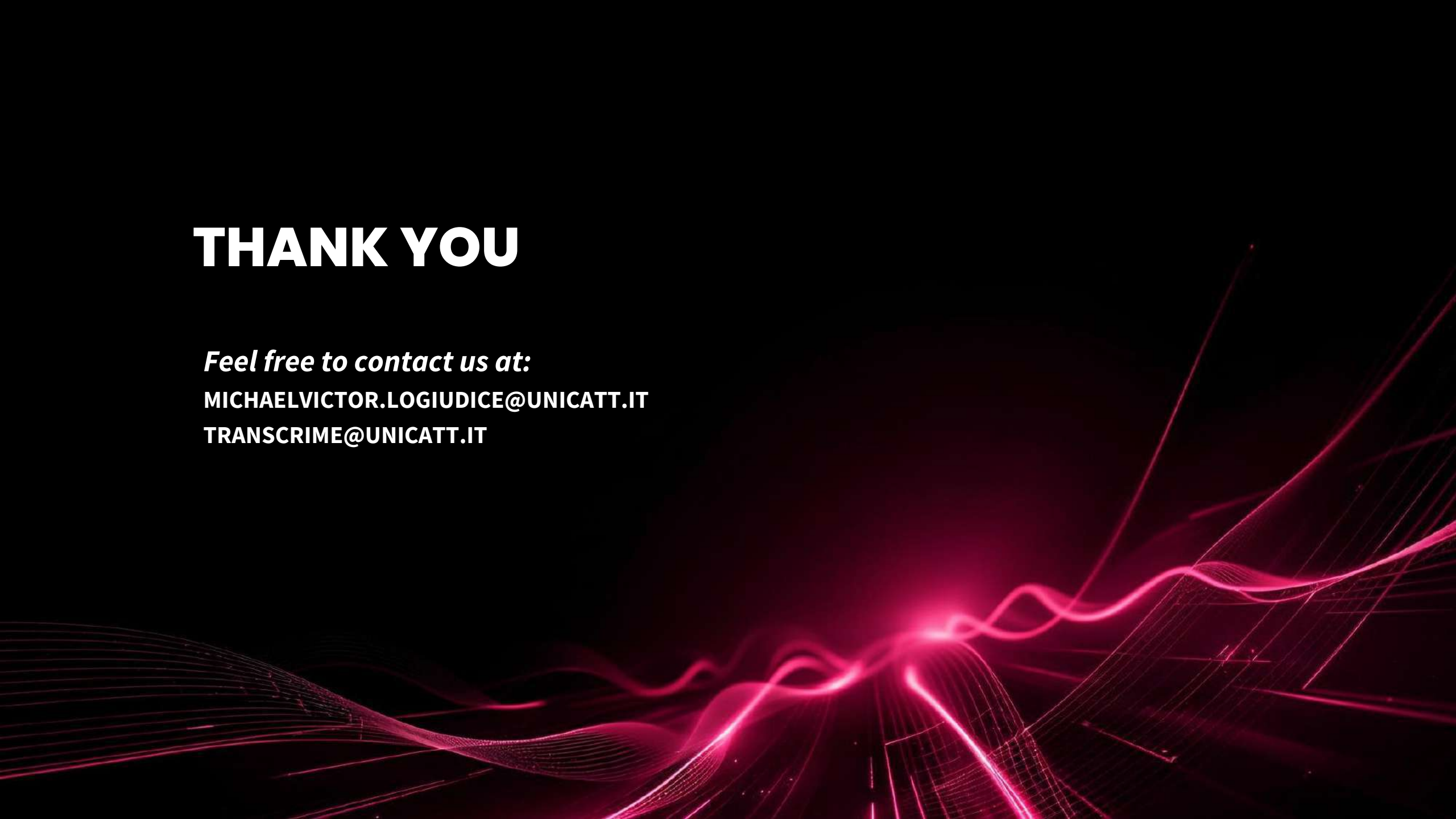
11.30	**Coffee Break**
11.40	**Session 3: Supply-Chain Vulnerabilities and Due Diligence** Lukasz Wojciechowski (Regnology)
12.25	**Session 4: The DATACROS III Toolbox** Michael Lo Giudice (Università Cattolica del Sacro Cuore - Transcrime)
12.50	**Q&A and Closing remarks**

data | cros^3 TRANSCRIME UNIVERSITÀ CATTOLICA del Sacro Cuore Regnology

THANK YOU

Feel free to contact us at:

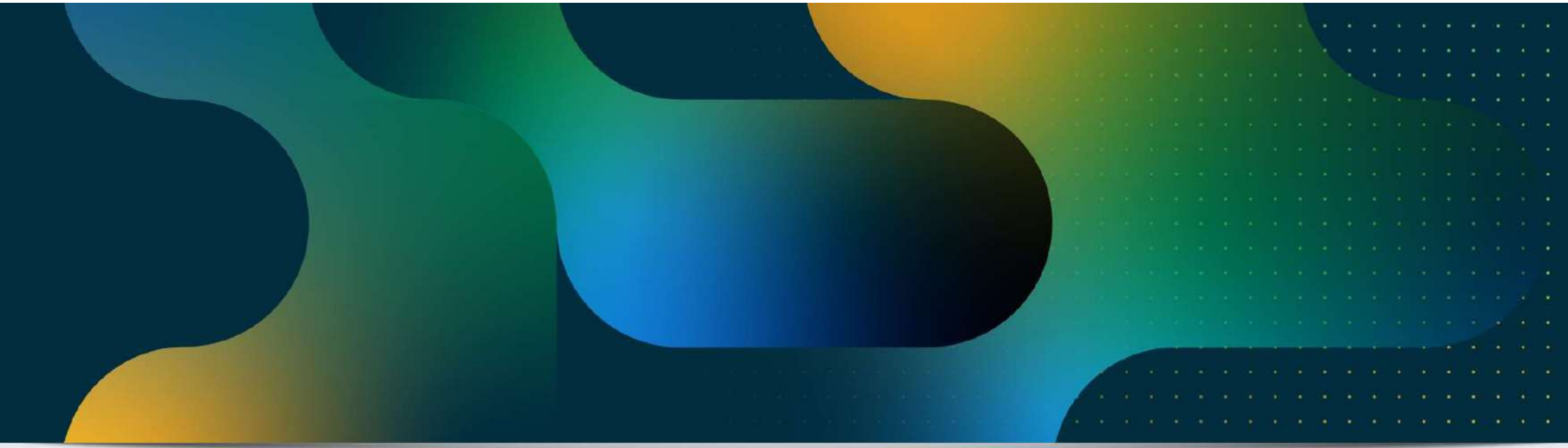
MICHAELVICTOR.LOGIUDICE@UNICATT.IT
TRANSCRIME@UNICATT.IT



Identifying criminal red flags in AML Due Diligence for high-risk customers and supply chains

Training for Banking, AML obliged entities and corporate sector

Regnology



About Regnology

ABOUT REGNOLOGY

Leveraging a global reach

Recognized as the world's leading RegTech and SupTech provider

100
Countries served across EMEA, APAC and the AMERICAS

30+
Offices with a presence in all key financial centers

1000+
Regulatory, Risk and Finance experts with decades of knowledge

13
Data Centers

Chartis RiskTech100 2026
Regnology
Regulatory Reporting: Banking

Chartis RiskTech100 2026
Regnology
Supervisory Tech (SupTech)

Chartis RiskTech100 2026
Regnology
Regulatory Reporting: Insurance

Risk Markets Technology Awards 2025
WINNER
Regulatory reporting product of the year
Regnology

waters Rankings Winner 2025
Best reporting system provider
Regnology

Regnology

SESSION 1: The Landscape of Organised Crime in the Corporate World

1 Defining Organised Crime | 2 The Sophisticated Infiltration of Legitimate Businesses | 3 Analysis of vulnerable sectors and the reasons for their targeting | 4 Key Real-World Examples

Regnology

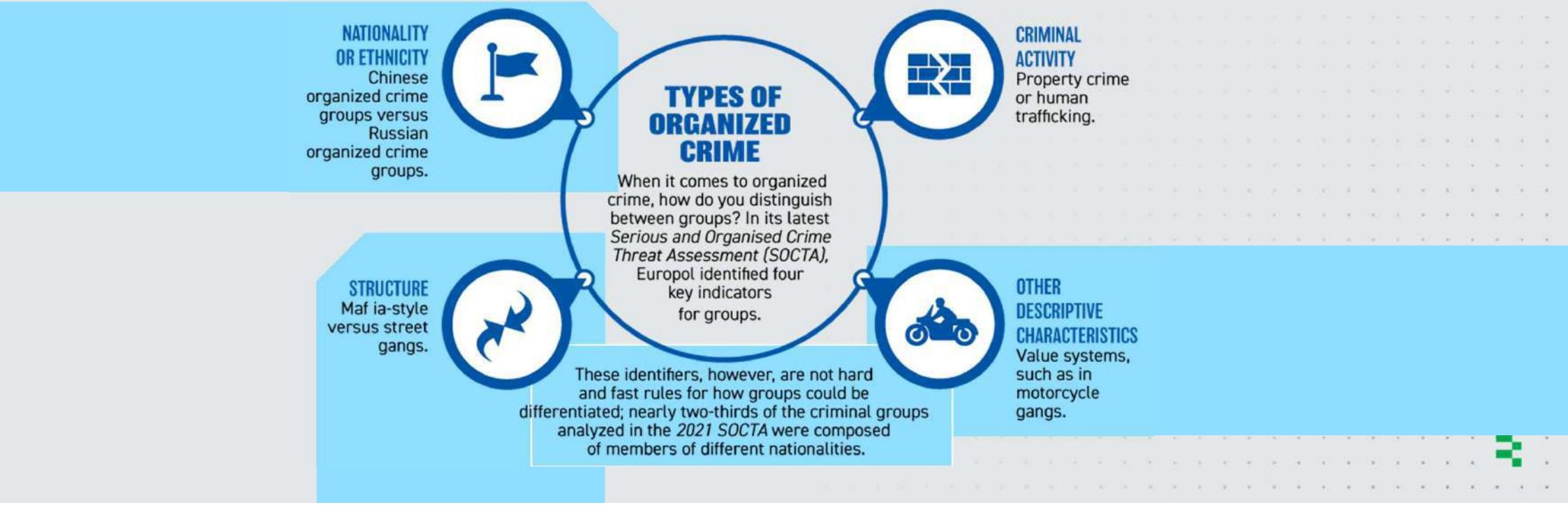
SESSION 1: The Landscape of Organised Crime in the Corporate World

1 Defining Organised Crime | 2 The Sophisticated Infiltration of Legitimate Businesses | 3 Analysis of vulnerable sectors and the reasons for their targeting | 4 Key Real-World Examples

Defining Organised Crime

What is (Modern) Organised Crime?

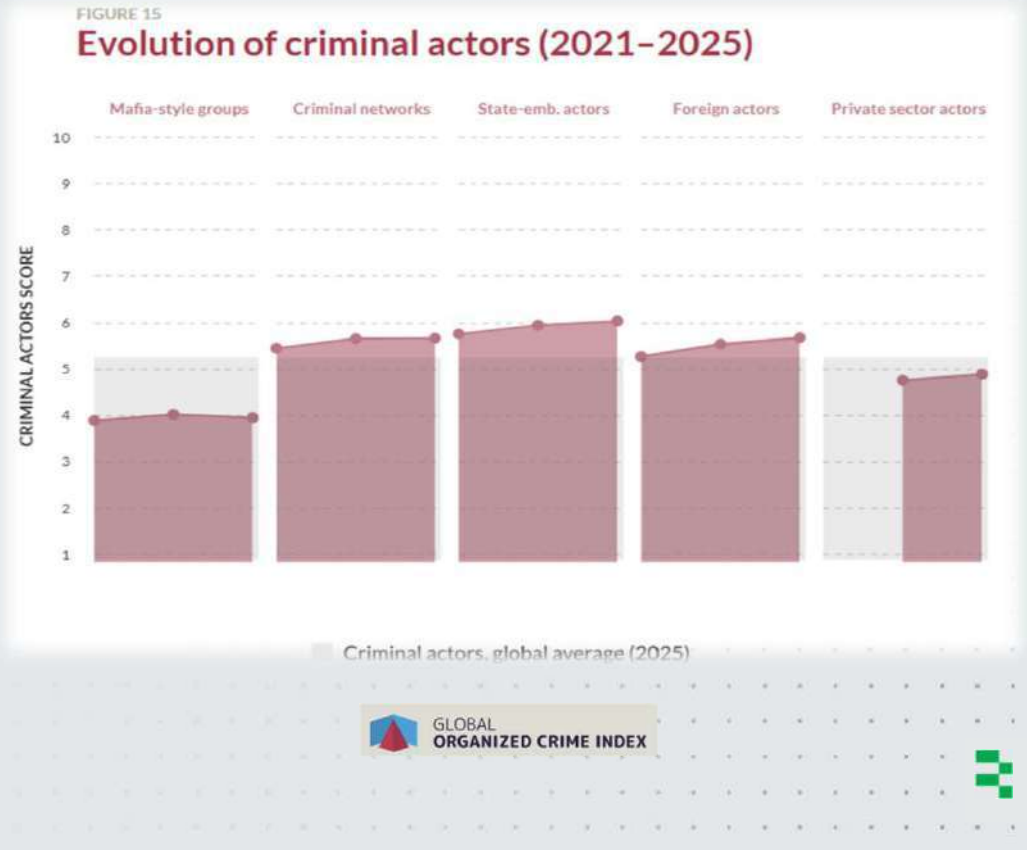
Organised crime refers to ~~centralised groups or~~ fluid networks, **operating locally, nationally, or transnationally**, that engage in **planned and coordinated** illegal activities, primarily for **financial or material benefit**. These groups are characterised by their continuing nature and often **employ corruption, violence**, and complex organisational structures to protect their Operations.



Defining Organised Crime

Beyond the Stereotype: Evolution of Organised Crime

The Old Model:	The Modern Reality:
The "Gangster" Stereotype	The "Illicit CEO"
Structure:	**Structure:**
Rigid & Hierarchical	Networked, Fluid & Decentralised
Focus:	**Focus:**
Local / Regional	Transnational / Global
Primary Driver:	**Primary Driver:**
Violence & Territory	Profit & Market Share
Analogy:	**Analogy:**
The Godfather	The Illicit Multinational Corporation



Defining Organised Crime

Beyond the Stereotype: The Changing DNA of Organised Crime

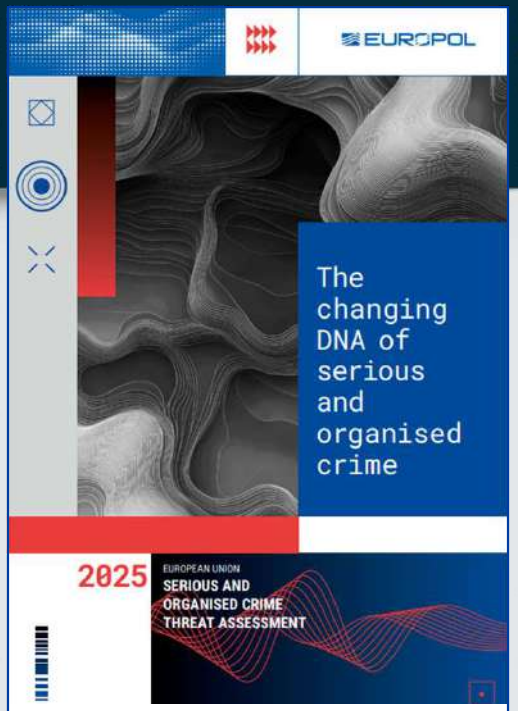
Just as DNA serves as the blueprint for life, we are seeing a fundamental shift in the 'blueprint' of crime.

Key transformations ("DNA" of crime)

- **Digitalisation**
  - More crimes are committed **online**.
  - The internet is a primary operating environment (fraud, cyberattacks, exploitation).
- **Technology (AI)**
  - AI and new technologies:
    - increase **scale and automation**
    - lower barriers to entry for criminals
- **Hybrid threats (links to state actors)**
  - Criminal groups:
    - cooperate with state-linked actors
    - act as **proxies in hybrid threats**
- **Destabilisation**
  - Dual effect:
    - **huge profits and parallel economies**
    - **corruption and erosion of institutions**

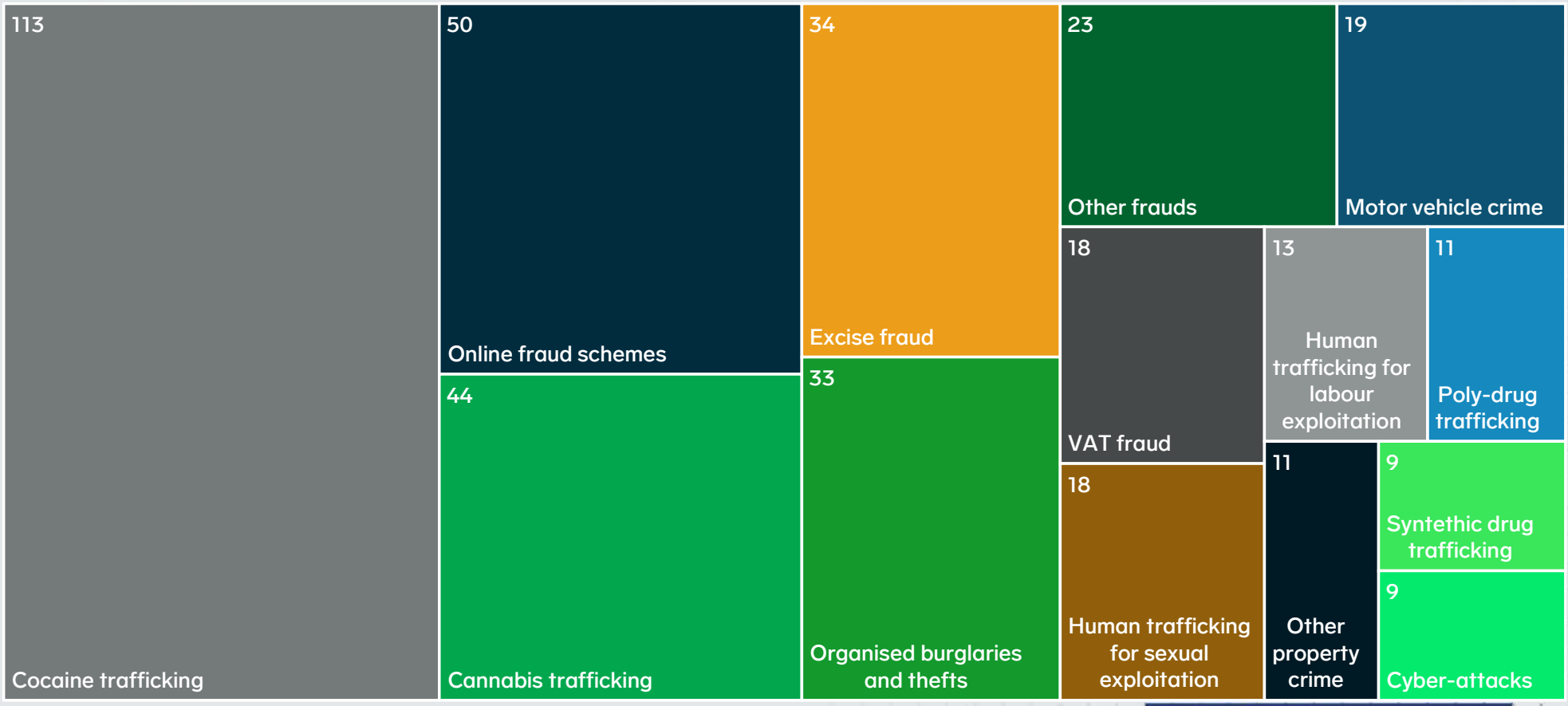
Characteristics of criminal networks

- More:
  - **flexible and network-based (non-hierarchical)**
  - **transnational**
- Strong use of:
  - encrypted communication
  - digital platforms
- Increasing convergence of crime types (e.g. cyber + drugs + money laundering)



- Europol's flagship report published every 4 years.
- Based on **thousands of investigations, EU Member State data, private sector input, and experts.**
- Purpose: identify the **main organised crime threats and their future development.**

Number of most threatening criminal networks involved in the different types of activities as a sole main activity

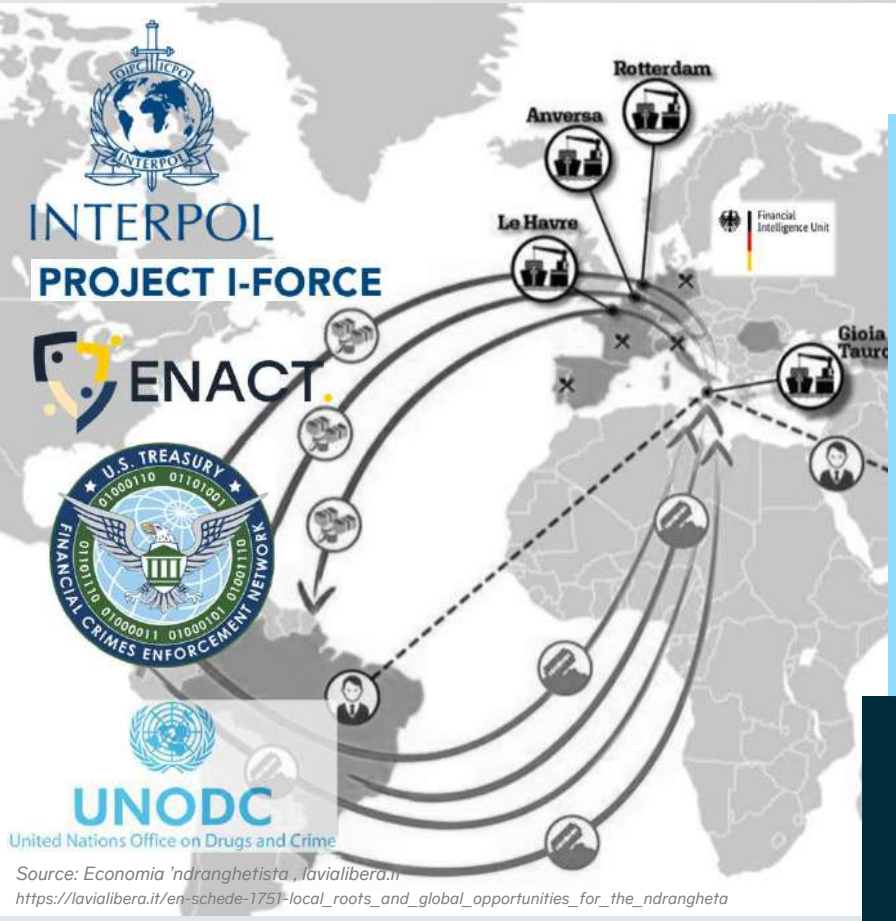


EUROPOL

DECODING THE EU'S MOST THREATENING CRIMINAL NETWORKS

Defining Transnational Organised Crime

The Global Reach



Source: Economia 'ndranghetista , lavialibera.it
https://lavialibera.it/en-schede-1751-local_roots_and_global_opportunities_for_the_ndrangheta

A Global Phenomenon – Borders Increase Value

Crossing international borders is a **huge multiplier for organised crime**, making their operations both more profitable and safer. The added risk and complexity of smuggling goods like drugs or weapons drive up the price on the other side, **creating a 'risk premium'** that lines their pockets.

At the same time, criminals exploit the gaps between different legal systems, **using one country as a safe base to target another**, knowing that police forces struggle to cooperate across jurisdictions.

The United Nations Convention against Transnational Organised Crime provides a framework for international cooperating to combat this threat.

Regnology

SESSION 1: The Landscape of Organised Crime in the Corporate World

1 Defining Organised Crime | 2 The Sophisticated Infiltration of Legitimate Businesses | 3 Analysis of vulnerable sectors and the reasons for their targeting | 4 Key Real-World Examples

Regnology

Key Statistics

Legal Economy Infiltration level

86% using LBS

63% of 86% setting up or infiltrating legal business structures or forcing insiders for access/control.

Source: Europol, 2024

Global Annual Proceeds

$3-5 trillion

Transnational organised crime generates $3-5 trillion annually – constituting to around 5% of global GDP.

Source: ICAIE. 2024

Money Laundering

2-5% of global GDP

$1.6 to 2 trillion laundered annually – 70% through global financial system.

Source: UNODC. 2018

Most Lucrative: Counterfeiting

$0.9-1.13 trillion

Most lucrative illegal activity estimated is Counterfeiting, fallowed by drug trafficking ($426-652 billion)

Source: GFI. 2017

Seizure Rate

~2% seized

Less then 2% of laundered money is seized annually.

Source: EUROPOL. 2022-2024

Global Impact

140+ countries

Organised crime affects over 140 countries worldwide. 76% are present or active in two to seven countries.

Source: UNODC. 2020, Europol 2024

The Sophisticated Infiltration of Legitimate Businesses

Primary Goals for Infiltrating Legal Economies

1

Economic Domination & Financial Security

❖ Money Laundering & Risk Mitigation

Launder illicit wealth through three stages: placement, layering, and integration.

- Acquire cash-intensive businesses (restaurants, retail) for placement
- Use complex transactions and real estate investments for layering and integration
- Hedge against volatility of illicit markets

❖ Market Monopolization

Establish monopolies in sectors like construction, waste management, or agriculture.

- Use illicit capital to undercut legitimate competitors
- Engage in coercive tactics to stifle entrepreneurship

2

Quest for Power & Social Control

❖ Social Legitimacy & Community Control

Cultivate a public persona of legitimate entrepreneurship and philanthropy

- Become significant local employers, fostering dependency and loyalty
- Create a protective social buffer, making residents less likely to cooperate with authorities

❖ Territorial Control & Parallel Governance

Provide essential services in areas where the state is weak to become a parallel power.

- Use violence and threats to endorse control

3

Political influence & Corruption

❖ Systemic Corruption

Use economic leverage from legitimate businesses for bribery and political relationships.

- Secure government contracts, obtain licenses, and influence legislation
- Gain warnings about investigations and influence judicial outcomes

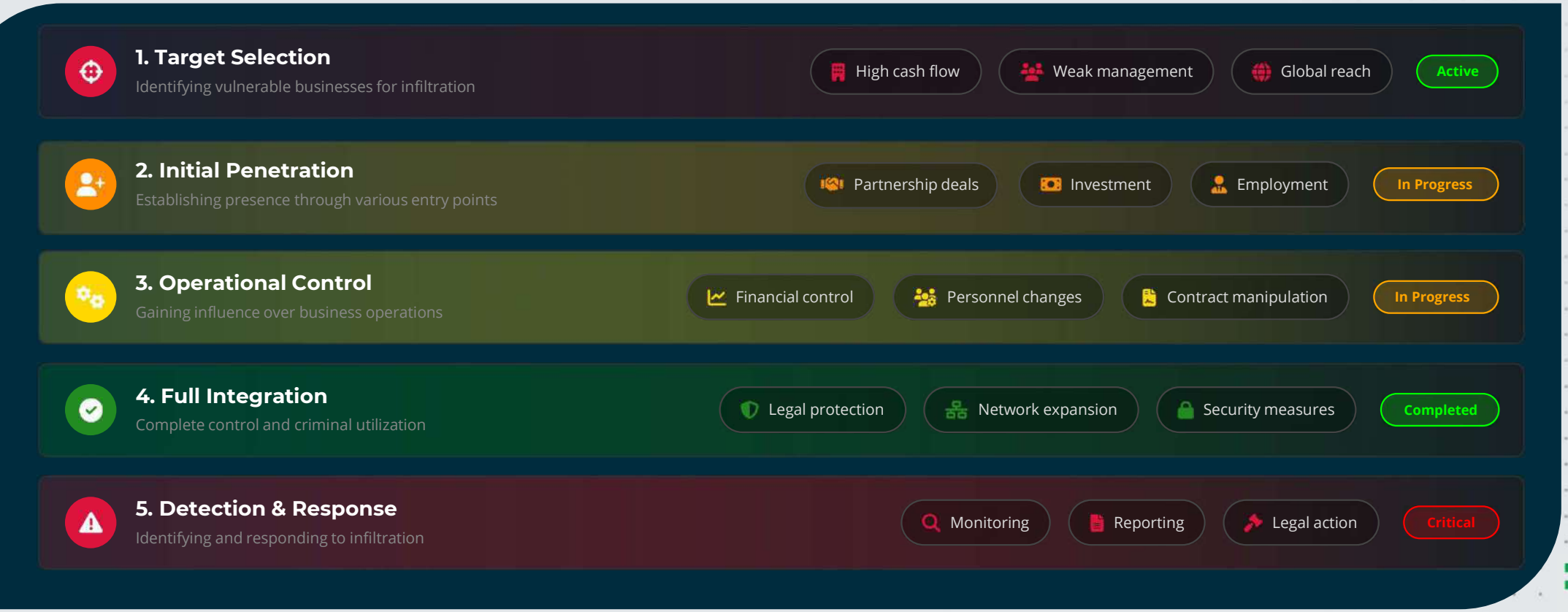
❖ State Capture

In its most advanced form, this can lead to a "mafia state."

- The lines between government and organised crime become fundamentally blurred

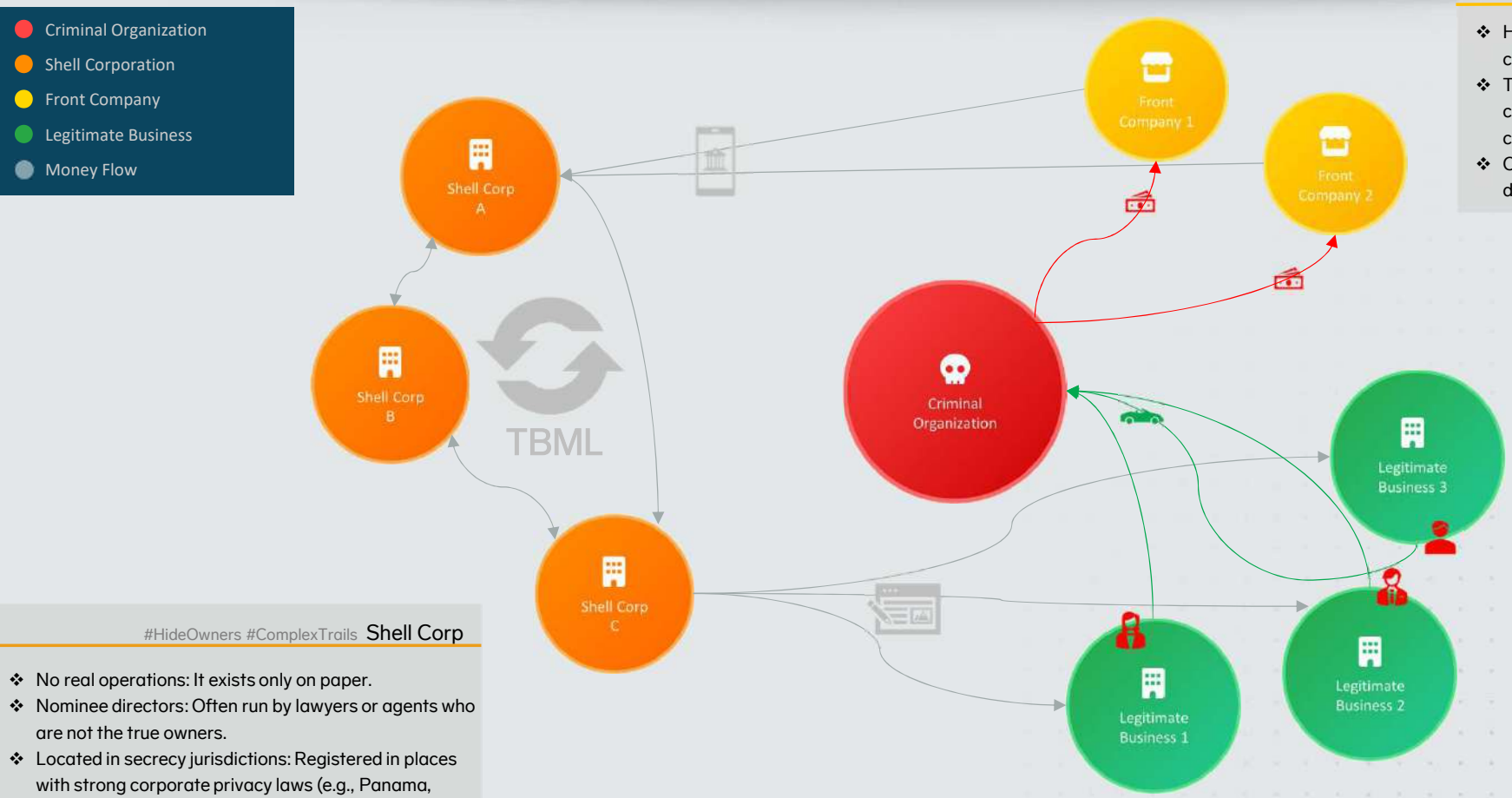
The Sophisticated Infiltration of Legitimate Businesses

Organised Crime Infiltration Process



The Sophisticated Infiltration of Legitimate Businesses

Criminal Organization Structure & Operation



Front Company #FinancialSystem #Cash Deposition

- Has real, day-to-day operations: It serves actual customers and generates some legitimate revenue.
- Typically cash-intensive: Businesses like restaurants, car washes, laundromats, bars, or construction companies are ideal.
- Commingles funds: Mixes illicit cash with legitimate daily earnings, making it hard to distinguish the source.

#HideOwners #ComplexTrails Shell Corp

- No real operations: It exists only on paper.
- Nominee directors: Often run by lawyers or agents who are not the true owners.
- Located in secrecy jurisdictions: Registered in places with strong corporate privacy laws (e.g., Panama, British Virgin Islands, Delaware) to make tracing ownership difficult.

Legitimate Business #CleanMoney #Assets

- A genuine, profitable enterprise: Often a well-established company with a good reputation.
- Can be any type of business: Real estate development, import/export, luxury goods, transportation, etc.
- The final destination for clean money: Used to purchase assets, pay salaries, and build a seemingly legal empire.

The Sophisticated Infiltration of Legitimate Businesses

A Closer Look at Infiltration Methods

1. Management Takeover

- **Forced Partnership:** Business owners pressured through threats or debt into accepting a criminal as a silent partner.
- **Nominee Directors:** "Clean front men" (lawyers, relatives) placed as official owners while criminals control from shadows.

2. Financial Traps

- **Debt Leverage:** Loan sharking targets struggling businesses, converting unpaid debt into an ownership stake.
- **Bankruptcy Fraud:** Criminals force bankruptcies to buy businesses cheap, then revive them with illicit funds.

3. Corruption & Manipulation

- **Corrupt Insiders:** Employees or managers secretly bribed to manipulate records or enable hidden criminal access.
- **Public Procurement:** Criminals rig bids, bribe officials, or intimidate rivals to win contracts and launder money.

4. Sector Vulnerabilities

- **Supply Chain Control:** Criminals control key suppliers or subcontractors, making the business unknowingly dependent.
- **Strategic Sector Targeting:** Focus on weakly regulated, cash-heavy sectors like hospitality, real estate, and waste management.

Regnology

The Landscape of Organised Crime in the Corporate World

1 Defining Organised Crime | 2 The Sophisticated Infiltration of Legitimate Businesses | 3 Analysis of vulnerable sectors and the reasons for their targeting | 4 Key Real-World Examples

Analysis of vulnerable sectors and the reasons for their targeting

Why the Financial Sector Is Targeted

- **Popularity:** Extremely High

Financial Gain as Core Object

Primary motivation

The **main objective of most OC is financial gain**. Criminals target the financial sector because it offers the most direct path to converting illicit proceeds into legitimate-looking assets.

Weaknesses in National Laws

Features

Weaknesses in national laws are a significant contributing factor to transnational financial crimes, enabling criminals to operate with reduced risk.

Transaction Volume Provides Cover

2-5% of global GDP

The **immense volume of daily transactions** provides cover for illicit funds, making it difficult to identify suspicious activity among millions of legitimate transactions

Regulatory Differences Vulnerability Exploited

Cross-border movement

Criminals **exploit differences in regulations between countries** to move money and obscure its origin, taking advantage of varying compliance standards.

Analysis of vulnerable sectors and the reasons for their targeting

Construction Infiltration

- **Popularity:** High

A Dual Objective of Profit and Laundering

Primary motivation

To **generate illicit profits** through extortion and bid-rigging, and to **launder large sums of money** through inflated project costs.

Methods of Industry Control

Features

Involves **labour racketeering, control of unions, bid-rigging on public contracts,** and forcing the use of mob-controlled suppliers.

Complexity as Concealment

Reasoning for Popularity

The **complexity and high value of projects, along with multiple layers of subcontracting**, create an opaque environment where fraud is difficult to detect.

Divers of Illicit Opportunity

Key Vulnerabilities

Fragmented regulatory oversight, a transient workforce, reliance on cash for wages, and susceptibility to intimidation.

Analysis of vulnerable sectors and the reasons for their targeting

Waste Management: Profiting from Pollution

- **Popularity:** Consistently high

Primary motivation for Profit

$10-$12 billion annually

To generate **profits through illegal dumping** of hazardous and commercial waste, and to establish monopolies through intimidation.

The Illicit Waste Cycle

Features

Price-fixing, **illegal dumping to avoid high disposal fees**, and infiltrating or creating legitimate-seeming disposal companies.

High Profits, Low Risk, and Weak Penalties

Reasoning for Popularity

It offers a **high-profit, low-risk criminal enterprise**. The cost of legal disposal is high, creating a profitable black market. Penalties are often low if caught.

Regulatory Gaps and Economic Incentives

Key Vulnerabilities

High costs of legal disposal, weak regulatory enforcement in some areas, and the difficulty of tracking waste from its source to its final destination.

Analysis of vulnerable sectors and the reasons for their targeting

Renewable Energy Vulnerability

- **Popularity:** Rapidly increasing

Exploiting Subsidies and Laundering

Primary motivation

To **exploit massive government subsidies** and to launder large sums of money through complex, high-value development projects.

Green Energy's Hidden Lure for Organised Crime

Features

Huge subsidies and project complexity enable financial crime. Additionally, the sector's **valuable, remote assets** are prime targets for organised theft.

Lucrative Complexity

Reasoning for Popularity

The sector's massive influx of funding and complex project structures make it a **lucrative yet hard-to-monitor target** for organised crime.

Triple Vulnerability

Key Vulnerabilities

Generous and often **poorly monitored subsidy programs**, the high capital cost and financial complexity of projects, **physical vulnerability** of large remote solar and wind farm to theft

Analysis of vulnerable sectors and the reasons for their targeting

Organised Crime in Real Estate

• **Popularity:** High

Primary motivation for Launder

43% of OC use to launder

To **launder very large sums of illicit money in single transactions** and to convert "dirty" money into a stable, appreciable asset.

Hiding Illicit Gains

Features

Involves the use of **anonymous shell companies and trusts, purchasing property with cash,** and "property flipping" to obscure the money trail.

Stability, Secrecy, and Scale

Reasoning for Popularity

High-value transactions can legitimize large amounts of cash at once. The investment is relatively stable, and **complex legal structures can easily hide the true ownership** of funds.

Real Estate's Blind Spots

Key Vulnerabilities

The use of intermediaries (like lawyers and agents) with **insufficient due diligence, private sales lacking transparency**, and weak beneficial ownership registries.

Analysis of vulnerable sectors and the reasons for their targeting

Logistics Under Siege

- **Popularity:** Very High

Distribution Hub

Primary motivation

To act as the physical distribution network for illegal goods (drugs, weapons, counterfeit items) and for human trafficking.

Methods of Exploitation

Features

Involves smuggling within legitimate cargo, outright theft of high-value goods, and corruption of employees within the supply chain.

Essential for All Criminal Logistics

Reasoning for Popularity

All criminal enterprises that deal in physical goods or people **require a method of transportation**. Criminals exploit existing, complex global supply chains.

Vulnerability Through Volume

> 2% physically inspected

The vast scale of global trade makes **comprehensive inspection impossible.** There is a reliance on numerous third-party actors and a susceptibility to insider threats.

Analysis of vulnerable sectors and the reasons for their targeting

Hospitality (Hotels, Restaurants, and Bars)

- **Popularity:** Moderately High

The Cash Cleanser and Criminal Cover

Primary motivation

To serve as a **classic vehicle for laundering** cash-intensive criminal proceeds and to act as a **physical front** for other illegal activities.

Blending Illicit Funds and Fronting Illegal Activities

Features

Mixing illicit cash with legitimate daily revenue, extorting "protection" money from owners, and using the business as a base for illegal gambling, prostitution, or drug sales.

Community Hubs & Criminal Gains

Reasoning for Popularity

High **daily cash volumes cover illegal fund mixing.** These businesses offer community foothold and are easily taken over during downturns.

Risk Magnets: High Cash, Transient Staff

Key Vulnerabilities

High reliance on cash, high staff turnover, and vulnerability to intimidation and extortion rackets.

Regnology

The Landscape of Organised Crime in the Corporate World

1 Defining Organised Crime | 2 The Sophisticated Infiltration of Legitimate Businesses | 3 Analysis of vulnerable sectors and the reasons for their targeting | 4 Key Real-World Examples

Regnology

Biggest Money Laundering Cases: Russian Laundromat

Key Real-World Examples

Key Real-World Examples

What Was the Russian Laundromat?

The Greatest Financial Fraud of the Decade

Exposed by the Organized Crime and Corruption Reporting Project (OCCRP), the "Russian Laundromat" was an intricate mechanism that moved vast amounts of illicit funds out of Russia between 2010 and 2014.

Massive Scale

The scheme successfully laundered an estimated **$20 Billion to $80 Billion**, funnelling wealth from Russian oligarchs, criminals, and corrupt politicians into the global financial system.

The Mechanism

The core of the operation relied not on physical smuggling, but on exploiting the legal system through fake debts, corrupt Moldovan judges, and complicit EU banks.

Verified Source:
OCCRP: "The Russian Laundromat Exposed"

Key Real-World Examples

Phase 1: Fictitious Loans & Shell Companies

Creating the illusion of legitimate international debt.

Step 1: The Fake Agreement

Two shell companies (often registered in the UK with hidden beneficial owners) would sign a contract for a massive, entirely fictitious loan—often in the hundreds of millions of dollars.

Step 2: The Guarantors

A Russian company (which secretly held the dirty rubles) and a Moldovan citizen (to ensure Moldovan court jurisdiction) were appointed as "guarantors" for this fabricated debt.

Step 3: The Planned Default

The "borrowing" shell company would deliberately default on the loan, legally triggering the obligation of the Russian and Moldovan guarantors to pay the massive debt.

Key Real-World Examples

Phase 2: Exploiting Moldovan Courts

Weaponizing the judicial system to launder funds.

Judicial Laundering

Once the "default" occurred, the creditor shell company sued the guarantors in a Moldovan court. Because a Moldovan citizen was listed on the contract, the local courts had jurisdiction.

The Corrupt Verdict

Complicit Moldovan judges ignored glaring red flags, authenticated the fake debts, and issued legally binding court orders demanding the Russian guarantor pay the UK shell company.

The Alibi

This court order provided the ultimate "legitimate" pretext. Banks rarely questioned funds moved to execute a formal, state-backed judicial ruling.

Key Real-World Examples

Phase 3: The European Gateway

Transforming dirty rubles into clean EU assets

Step	Institution	Laundering Action
1	Moldindconbank (Moldova)	Received massive deposits of dirty rubles from the Russian company under the strict guise of fulfilling the court-ordered debt repayment.
2	Trasta Komercbanka (Latvia)	**Funds were instantly wired here. Since Latvia is in the EU, the money entering this bank formally crossed into the European financial system, acquiring legitimacy.**
3	Global Correspondent Banks	Once parked in an EU bank, the 'clean' funds were swiftly dispersed across the globe through standard correspondent banking networks.

Key Real-World Examples

Russian Laundromat

- Criminal Organization
- Shell Corporation
- Front Company
- Legitimate Business
- Money Flow

TKB Trasta komercbanka

ŪKIO BANKAS

Danske Bank

Русский Земельный Банк

Royal Bank of Scotland

5.3

citi

Deutsche Bank

HSBC

37.1

MOLDINDCONBANK

OCCRP | Organized Crime and Corruption Reporting Project

Key Real-World Examples

AML/CDD Red Flags That Were Ignored

Clear indicators of illicit finance that compliance teams missed.

Illogical Jurisdictions

Massive, round-dollar transfers executing court judgments from inherently high-risk jurisdictions (Moldova) flowing directly into offshore accounts via a third country (Latvia).

Obscured Ownership

Ultimate Beneficial Owners (UBOs) for the involved entities were completely hidden behind layers of anonymous UK Limited Liability Partnerships (LLPs) and offshore shell companies.

No Economic Rationale

Zero commercial justification for the underlying transactions. Why would an obscure UK shell company lend $500 million to another shell company, backed by a random Moldovan citizen?

Regnology

Laundering Proceeds via Subsidized Wind Power: The Renewable Energy Sector infiltration

Key Real-World Examples

Why the Mafia Targets Renewables

Transitioning to the Legitimate Economy

Organized crime groups are diversifying from extortion and traditional crime into highly subsidized, modern economic sectors.

Lucrative Subsidies

Generous EU and state-level green energy certificates provide guaranteed, long-term returns on investment, maximizing profits.

Ultimate Money Laundering

Wind farms are massively capital-intensive infrastructure projects. They serve as the perfect vehicle to absorb and wash billions in illicit drug proceeds.

The Green Laundering Mechanism

Transforming cocaine revenue into state-subsidized clean energy.

Step 1: Illicit Capital Injection

Vast proceeds generated from international drug trafficking are injected into the legitimate economy to fund the initial massive capital costs of wind farm construction.

Step 2: Corrupted Permitting

The syndicate bribes local officials, mayors, and zoning boards to expedite environmental permits and acquire strategic, windy land tracts seamlessly.

Step 3: The "Clean" Wash

The energy produced is sold into the national grid. The revenue returned—alongside lucrative public subsidies—is now completely clean, legitimate money.

Europe's Largest Wind Farm

The 'Ndrangheta Arena clan's infiltration of Isola di Capo Rizzuto.

The €350 Million Seizure

In a massive anti-mafia operation, Italian authorities seized what was then considered one of Europe's largest wind farms in Calabria, valued at **€350 million**.

Corporate Obfuscation

The incredibly powerful **Arena clan** infiltrated the project using a vast, untraceable network of foreign bank accounts and shell companies based in San Marino, Germany, and Switzerland.

The Prosecutor's Verdict

Renowned Anti-Mafia prosecutor Nicola Gratteri confirmed the wind park was built fundamentally as a vehicle to wash immense proceeds generated from cocaine trafficking.

AML/CDD Red Flags in Subsidized Sectors

Applying lessons learned to enhance institutional defense.

Unjustified Capital

Sudden, massive injections of previously unknown capital into heavily subsidized infrastructure projects by entities lacking a track record in the sector.

Hidden Ownership

Project developers, contractors, or investment vehicles relying on completely hidden Ultimate Beneficial Owners (UBOs) located in known offshore tax havens.

Suspicious Fast-Tracking

Unusually rapid approval of highly restrictive land rights and environmental permits, especially when involving local or regional Politically Exposed Persons (PEPs).

Regnology

Crypto Laundering: Unmasking Darknet Mixers and Digital Smuggling

Key Real-World Examples

Case: The Helix Darknet Mixer

Laundering 350,000 Bitcoins for the digital underworld.

The DOJ's $400M Takedown

The U.S. Department of Justice secured the forfeiture of over **$400 million** in assets tied to Helix, a notoriously infamous cryptocurrency "mixer" operating on the darknet.

The Operator

Operated by Larry Dean Harmon from 2014 to 2017, Helix was specifically designed to obscure the blockchain trail for users of illegal darknet marketplaces.

The Scale

During its operation, Helix successfully laundered over **350,000 Bitcoins**—representing hundreds of millions of dollars in drug proceeds.

How Darknet Mixers Work

Obscuring the blockchain ledger to evade forensic tracking.

The "Tumbler" Concept

Cryptocurrency Mixers (or Tumblers) are services specifically designed to break the transparent link between a sender's and receiver's crypto addresses.

- **Inputs:** Criminals deposit traceably "dirty" Bitcoin into the mixer's massive central pool.
- **Mixing:** The algorithm fragments, delays, and endlessly scrambles the coins with clean funds from thousands of other users.
- **Outputs:** The user receives the equivalent amount in completely unrelated, disconnected Bitcoin to a fresh wallet.

AML/CDD Red Flags in Crypto

Identifying suspicious digital footprints for compliance teams.

Chain Hopping

Funds are rapidly exchanged across completely different blockchains (e.g., Bitcoin to Monero, then to Ethereum) specifically to break forensic tracing tools.

Mixer Exposure

Inbound transfers directly originating from known high-risk tumbler addresses or smart contracts, signaling an explicit intent to hide origin.

KYC Evasion Tactics

Utilization of nested accounts, structuring transfers just below KYC thresholds ("smurfing"), or relying exclusively on unregulated P2P exchanges.

Actionable Insight: Integrating blockchain analytics tools is now mandatory for institutions handling crypto off-ramps.

SESSION 1: The Landscape of Organised Crime in the Corporate World

Session 1 – Key Takeaways

86%

of the most threatening OC networks in the EU use legal business structures.

"Illicit CEOs"

Traditional stereotypes of Organised Crime are outdated. Today's criminals operate as corporate executives pursuing power, control, and legitimacy.

01 Organised Crime no longer operates “outside” the economy — it **operates through** it.

02 **86%** of the most threatening OC networks in the EU use legal business structures.

03 The main goal is not only money laundering, but also **power, control and legitimacy**.

04 Early detection starts with recognising **corporate red flags** during onboarding and CDD.

05 Traditional stereotypes of OC are outdated — today we face “**Illicit CEOs**”.

→ **Now that we understand the threat landscape, let’s move to Session 2: How to detect these indicators in practice during Customer Due Diligence.**

Regnology

SESSION 2: Early Warning Indicators in Customer Due Diligence (CDD)

1 Methods of Enhanced Due Diligence (EDD) on high-risk customers | 2 Identifying behavioural red flags and suspicious transactional patterns | 3 The role of technology in automating detection

Regnology

SESSION 2: Early Warning Indicators in Customer Due Diligence (CDD)

1 Methods of Enhanced Due Diligence (EDD) on high-risk customers

2 Identifying behavioural red flags and suspicious transactional patterns

3 The role of technology in automating detection

Methods of Enhanced Due Diligence (EDD) on high-risk customers

AML EU package: Regulatory compliance in the financial sector

Customer identification and beneficial owner (UBO)

Make sure the institution knows who the client truly is.

Ongoing transaction monitoring

Detects unusual or suspicious activity in real time or retrospectively

Reporting suspicious transactions to the Financial Information Unit (e.g., GIIF in Poland)

Mandatory escalation of AML/TF suspicions

Tipping-off ban (disclosure of reports)

Clients must not be informed about failed suspicious activity reports.

AML risk assessment and internal procedures

Institution-wide framework based on the risk-based approach

Data retention (min 5 years)

Retention of Know Your Customer and transaction data for regulatory access

Reporting obligations to supervisory authorities

Periodic reporting to the supervisory authority on AML controls and exposure

CONTINUOUS COMPLIANCE

Adhering to strict EU regulatory standards to ensure secure and transparent financial operations.

SECURITY FIRST

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Core AML/CFT Components

01
Designate a Compliance Officer

- Appointing an AML lead,
- Grant authority
- Make them the main contact for regulators

METHODOLOGY & RISK

02
Develop internal Controls

- Written AML Policies
- Risk-based procedures
- SAR and CTR processes

IDENTITY & KYC

03
Establish an AML Compliance Training Program

- Role-based training
- Red flag awareness
- Ongoing updates

OVERSIGHT & STR

04
Have Independent Audits of the Program Done

- Periodic AML Testing Control Effectiveness Review
- Corrective Actions

STAFF COMPETENCE

05
Perform Customer Due Diligence

- Customer identification, KYC, risk profiling
- ongoing monitoring

GOVERNANCE & AUDIT

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Criminal Typologies for Financial Crime Detection

AML Fundamentals

Understanding the three stages: placement, layering, and integration. Predicate offenses include fraud, trafficking, and cybercrime.

- **Placement** — Initial deposit
- **Layering** — Complex transfers
- **Integration** — Legitimate use

Risk-Based Approach (RBA)

FATF principle: Identify, assess, and understand ML risks, apply proportionate mitigation measures.

- **RBA** — Risk assessment
- **CDD** — Customer verification

CDD Tiers

Levels of due diligence: Simplified (SDD), Standard (CDD), Enhanced (EDD).

- **SDD** — Simplified checks
- **CDD** — Standard verification
- **EDD** — Enhanced review

Regulatory Frameworks

- **FATF** — Global standards
- **EU AMLDs** — EU directives
- **US CTA/BOI** — Beneficial ownership
- **EU CSDDD** — Supply chain

Technology & AI/ML

- AI/ML for behaviour analysis and anomaly detection
- Network analysis for relationship mapping

Methods of Enhanced Due Diligence (EDD) on high-risk customers

What is Enhanced Due Diligence

Definition

Enhanced scrutiny and risk assessment procedures conducted by financial institutions to analyse and verify high-risk accounts.

Purpose

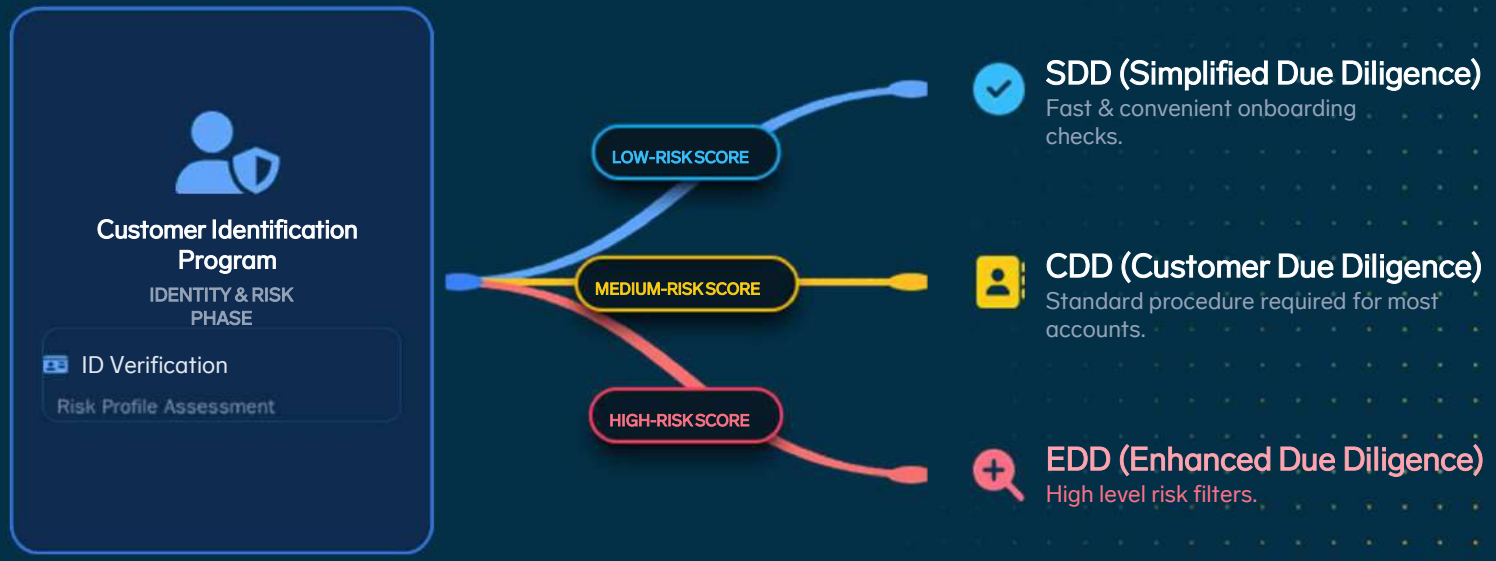
1. Mitigate risks with high-risk customers or jurisdictions.
2. Strengthen AML, KYC, and FATF compliance.
3. Safeguard financial institutions against fraud.

Scope

SDD: Low risk, simplified checks.
CDD: Medium risk, standard monitoring.
EDD: High risk, deep investigation.

CDD vs EDD: Tiers of Due Diligence

Customer onboarding routes profiles dynamically based on their analysed risk scoring from Customer Identification Program.



Methods of Enhanced Due Diligence (EDD) on high-risk customers

Entities obliged to apply AML/CFT measures

- **Financial Institutions** — banks, credit institutions, investment firms, insurers, currency exchanges, payment service providers, Virtual Asset Service Providers (VASPs), etc.
- **DNFBPs (Designated Non-Financial Businesses and Professions)** — so-called "gatekeepers":
  - Casinos and gambling operators,
  - Real estate agents,
  - Dealers in precious metals, gemstones, and works of art,
  - Lawyers, legal advisors, notaries (for specific transactions),
  - Certified auditors, tax advisors, accounting firms,
  - Providers of company formation services, trusts, and company service providers.

These entities must use CDD when (1) establishing a business relationship, (2) for occasional transactions above thresholds (usually 10,000 EUR/USD), (3) when there is suspicion of ML/TF, or when there are (4) doubts about the veracity or adequacy of previously obtained customer identification data.

AMLD/AMLR: Additionally, it includes crowdfunding, some NFT/crypto platforms, (high value) football clubs, etc.

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Mandatory AML/CFT Regulatory Reporting Obligations

01

Suspicious Transaction / Activity Reporting (STR/SAR)

- **Trigger:** knowledge, suspicion or reasonable grounds to suspect ML/TF — regardless of amount.
- **Full scope:** covers suspicious activity & behaviour, not only executed transactions.
- **Also includes:** attempted transactions and suspicions from inability to complete CDD.
- **Delivery:** reported directly to the national FIU (GIIF in Poland).

STR / SAR REPORTING

02

Threshold & Cash Reporting

- **Rule-based:** triggered automatically once a defined threshold is crossed — not risk-based.
- **EU cash limit:** cash payments above €10,000 prohibited in business (Member States may set lower).
- **Mechanism:** mandatory, mechanical escalation of large/defined flows. (US equivalent: CTR)

THRESHOLD REPORTING

03

UBO Registry Reporting

- **Transparency:** identify the ultimate beneficial owners behind clients and firms.
- **Registry filing:** report ownership structures to central beneficial-owner registers.
- **Maintenance:** keep data accurate; report changes of ownership on an ongoing basis.

UBO REPORTING

04

Sanctions Screening & Freezing

- **Screening:** monitor matches against EU and UN lists (US/OFAC where applicable).
- **Action:** implement immediate asset freezes on confirmed matches.
- **Reporting:** report freezes and any breaches to the competent authority.

SANCTIONS

Methods of Enhanced Due Diligence (EDD) on high-risk customers

When EDD Is Required

High-Risk Customers, such as:

- **(FATF R.12) Foreign Politically Exposed Persons (PEPs):** Public officials potentially vulnerable to corruption risks.
- **Offshore Accounts:** Often linked to opaque ownership structures.
- **Corporate Vehicles:** Entities with complex beneficial ownership.

High-Risk Jurisdictions: EDD is required for transactions or clients from regions with weak AML controls, such as FATF grey list countries.

Suspicious Behaviour or Adverse Media: Indicators like sudden large transactions, unusual activity, or media links to financial crimes often trigger EDD.

ONBOARDING CHECK

TYPES OF POLITICALLY EXPOSED PERSONS (PEPS)

1	2	3	4
Foreign PEPs	Domestic PEPs	International Organisation PEPs	Family Members
OVERSEAS	NATIONAL	INSTITUTIONS	ASSOCIATES

Defined under FATF Recommendation 12 as individuals entrusted with prominent public functions.

FATF

High-Risk Jurisdictions subject to a Call for Action (13 Feb 2026): Democratic People's Republic of Korea | Iran | Myanmar

JURISDICTIONS UNDER INCREASED MONITORING (13 FEB 2026): Algeria | Angola | Bolivia | Bulgaria | Cameroon | Côte d'Ivoire | DR Congo | Haiti | Kenya | Kuwait | Lao PDR | Lebanon | Monaco | Namibia | Nepal | Papua New Guinea | South Sudan | Syria | Venezuela | Vietnam | Virgin Islands (UK) | Yemen

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Key Methods of Enhanced Due Diligence

	Method.	Description
1	**In-depth Customer Verification**	Solid identification and verification of customer plus UBO
2	**Background checks.**	Check against PEP, sanctions, adverse media and reputational risk.
3	**Understanding Purpose and Nature**	Key question: Reasoning behind client approach, also expected nature of the relationship. Creating baseline
4	**Source of funds and wealth**	After understanding the objective, we verify the origin of the funds and wealth.
5	**Site visits**	Additional confirmation on-site corporate clients mostly
6	**Ongoing monitoring**	Intensive continuous monitoring after onboarding.

Recommended by:

FATF

the Wolfsberg Group

AML ANTI-MONEY LAUNDERING DIRECTIVES

Methods of Enhanced Due Diligence (EDD) on high-risk customers

In-Depth Customer Verification

Objective: To build a **comprehensive and verified profile** of a high-risk customer, moving beyond standard due diligence checks to mitigate potential risks.

	Identity Verification	Beneficial ownership	Business Profile
EDD	Collect additional information and apply more stringent verification measures, such as requiring multiple documents, certified copies, or using biometric checks.	Conduct a deeper investigation to understand the full ownership and control structure, especially if it is complex, to ensure the true individuals behind the entity are identified and verified.	Obtain more extensive information on the customer's business activities, expected transaction patterns, and examine the legitimacy and consistency of their business profile and financial history.
CDD	Verify name, address, and date of birth using reliable, independent source documents, data, or information.	Identify the ultimate beneficial owner(s) (UBOs) and take reasonable measures to verify their identity.	Understand the nature and purpose of the intended business relationship to develop a customer profile.

High Risk
In-depth verification

Low-Medium Risk
Basic verification

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Background Checks

Objective: to corroborate **declared information** and identify **undisclosed financial crime risks** or **reputational concerns** by scrutinizing external public sources and intelligence.

Effective background checks, especially for high-risk customers, follow a systematic process to uncover critical information. This can be conceptualised in three streamlined stages:

Screening: Identify Potential Red Flags

- Check the customer against sanctions list, PEP databases, and adverse media sources **to uncover potential red flags.**

Analysis: Evaluate and Verify Findings

- Review the initial findings to discard false positives and **confirm the relevance and credibility** of any true matches.

Action: Integrate and Decide

- Incorporate the verified findings into the customer's risk profile to make an informed decision **to accept, reject, or investigate further.**

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Understanding Purpose and Nature

Objective: to establish the legitimate business or economic **rationale for the relationship,** thereby creating a **baseline for expected activity** and assessing inherent risks.

KEY AREAS OF INQUIRY:

- What is the customer's stated economic objective?
- Does the rationale align with the customer's known business or industry?
- Why has the customer chosen this institution and these specific products?
- Who are the primary expected counterparties (senders and beneficiaries)?
- What are the anticipated geographic flows of funds (countries of origin and destination)?
- What are the expected transaction types, values, and frequency?

The Purpose of the Relationship

The Intended Nature of Activity

Outcome:

A well-defined and plausible **activity profile that serves as the benchmark** for detecting suspicious deviations during ongoing monitoring.

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Source of Funds and Wealth

Objective: to create a credible and verified **financial baseline for each customer.**

Feature	Source of Funds (SoF)	Source of Wealth (SoW)
Definition	The origin of the specific money or assets being used for a particular transaction.	The origin of a customer's entire body of assets or their total net worth.
Focus	Specific and transactional.	Holistic and biographical.
Key Question	Where did the money for this transaction come from?	How did this customer accumulate their entire fortune?
Scope	**Narrow**; focused on a single event or a series of related transactions.	**Broad**; encompasses the customer's overall economic profile and financial history.
Purpose	To verify the legitimacy of the funds being used in the immediate transaction.	To build a comprehensive risk profile and understand the customer's financial background.
Verification documents	Recent payslips, employment contract, bank statements, copy of the will (inheritance), loan agreement, brokerage account statement.	Audited financial statements, shareholder registries, statements from wealth managers/brokerage firms, property valuations, rental agreements, long-term view of declared income and assets, title deeds, probate documents

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Site Visits

Objective: **to physically verify a customer's operational reality and enhance risk assessment where documentation alone is deemed insufficient.**

Widely accepted practice for financial institutions to use site visits as part of their EDD toolkit for certain high-risk scenarios.

Triggers for a Site Visit

Business Profile

- The customer operates in a high-risk sector (e.g., cash-intensive business) or has a complex, opaque ownership structure.

Geographic Risk

The customer's primary operations are based in a jurisdiction known for high corruption levels or weak AML enforcement.

Verification Issues

Significant difficulties arise in verifying the information provided by the customer through other means.

Inconsistencies

The customer's declared business activity appears inconsistent with their transaction patterns or other known information.

Methods of Enhanced Due Diligence (EDD) on high-risk customers

Ongoing Monitoring

Objective: to ensure that the understanding of the customer's risk profile **remains current** and to **detect** any activity that is inconsistent with the established financial **baseline (Purpose & Nature + SoF/SoW).**

This is a **proactive and resource-intensive** process.

Element	Objective	How it Works
Real-Time Transaction Analysis	Prevent illicit activities before they complete.	Monitors transactions as they occur, using AI and behavioural profiling to instantly flag deviations from normal customer behaviour or predefined rules.
Continuous Risk Assessment	Maintain an always-current customer risk profile.	Dynamically adjusts customer risk scores based on ongoing activities, new information (e.g., from external feeds), and event-driven triggers.
Periodic Review / KYC Refresh	Keep CDD data complete and up to date.	Scheduled re-verification of customer data and documents, more frequent for high-risk clients, re-confirming the SoF/SoW baseline.

Regnology

SESSION 2: Early Warning Indicators in Customer Due Diligence (CDD)

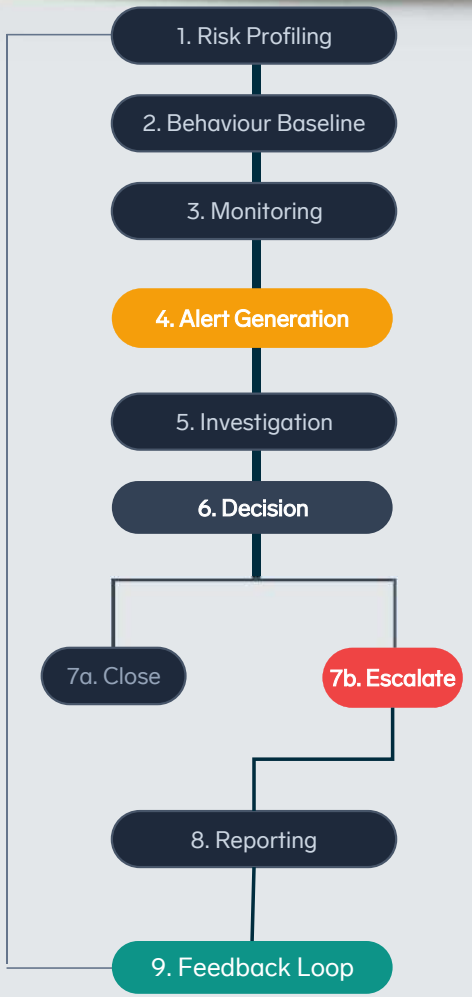
1 Methods of Enhanced Due Diligence (EDD) on high-risk customers |

2 Identifying behavioural red flags and suspicious transactional patterns

| 3 The role of technology in automating detection

Identifying behavioural red flags and suspicious transactional patterns

Action Framework: Behavioural Red Flags & Suspicious Transaction Monitoring



Objective	Key Activities	Red Flags / Patterns	Output
Understand risk level	KYC, CDD, risk scoring	High-risk country, complex ownership, PEP	**Customer rating**
Define "normal" activity	Analyse historical transactions	Typical size, frequency, geography	**Behaviour profile**
Detect anomalies	Rule-based & behavioural	Thresholds, unusual timing, velocity spikes	**Detection logic**
Flag suspicious activity	Automated alerts triggered	Structuring, rapid flow, unusual counterparties	**Alerts / cases**
Assess legitimacy	Review history & profile	Inconsistent activity, unclear source of funds	**Case decision**
Handle confirmed suspicion	Internal escalation, review	Strong indicators of laundering or fraud	**Escalated case**
Meet regulatory obligations	File STRs	Confirmed suspicious pattern	**Regulatory report**
Improve system	Tune rules, update models	Reduce false positives, adapt to new patterns	**Optimized system**

Identifying behavioural red flags and suspicious transactional patterns

Identifying Red Flags: Automation of Detection

Not all risk indicators are intended for system automation. To build an effective defence, we distinguish two fundamental groups of red flags based on their suitability for automated detection:

GROUP 01 // MANUAL REVIEW

Behavioural Red Flags

Nuanced, context-dependent cues that rely on experienced human judgement. They can be AI-assisted, but are hard to detect through automation alone.

.

REQUIRES HUMAN JUDGEMENT

- Third-Party Control
- Evasiveness
- Reluctance
- Undue Urgency
- Unusual Knowledge

GROUP 02 // SYSTEM MONITORING

Transactional Patterns

Perfect candidates for system-wide automation, algorithms, and real-time transaction rules, as they are based strictly on objective, structured, and quantifiable data points.

PRIME AUTOMATION CANDIDATES

- Location
- Amounts
- Frequency
- Velocity
- Counterparties

Identifying behavioural red flags and suspicious transactional patterns

Where To Look For Red Flags

Transactions

amounts, frequency, or destinations

Customer behaviour

reluctance, cooperation, consistency

Documentation

consistency, presence, reflecting reality

Business operations

ownership & structure characteristics

Geographic risk

high-risk countries and jurisdictions

Products/services

consistency with business, risk level aligned

Identifying behavioural red flags and suspicious transactional patterns

Key High-Risk Customer Profiles and Activities

Politically Exposed Persons (PEPs)

Individuals holding prominent public functions, and their associates, present severe bribery and corruption risks.

High-Risk Jurisdictions

Entities connected to countries with weak AML regimes, high corruption, or subject to strict international sanctions.

Complex Business Structures

Intricate ownership models, shell companies, and trusts designed to actively obscure ultimate beneficial owners.

Unusual Transaction Patterns

Activities that are unexpectedly large, rapidly sequenced, or completely lack apparent economic or lawful purpose.

Inconsistent Information

Customer's continuous reluctance to provide details or glaring discrepancies in onboarding documentation.

Cash-Intensive Businesses

Operations dealing heavily in physical cash, such as MSBs and pawnshops, making tracing inherently difficult.

Virtual Asset Sector

The decentralised and pseudonymous nature of cryptocurrencies attracts sophisticated laundering attempts.

Non-Resident / Offshore

Customers crossing multi-jurisdictional borders, greatly compounding the difficulty of verifying authentic identities.

High-Net-Worth Individuals

Wealthy individuals in connection with other suspicious factors such as complex structures, offshore private banking, and large volumes.

Other High-Risk Categories

Broad threats including cross-border NPOs, unexplained adverse media presence, or suspected criminal links.

Identifying behavioural red flags and suspicious transactional patterns

Identifying Suspicious Corporate Clients: Legitimate vs Red-Flag Patterns

Legitimate		Red Flag
Transparent Accounts Regular independent audits, proper records, and clear financial accounting.	FINANCIAL MANAGEMENT	**Complex/Cash-Heavy Operations** Irregular high-volume flows, missing documentation, and no audit trails.
Clear Structure Verified shareholders, direct ownership paths, and open hierarchy.	OWNERSHIP STRUCTURE	**Hidden/Unclear Beneficiaries** Complex shell companies, proxy owners, and opaque corporate layers.
Professional Management Culture Standard hiring practices, formal contracts, and labour law compliance.	EMPLOYEE RELATIONS	**High Staff Turnover** Unusual hiring patterns, fear-based management, and high staff turnover.
Complete Records Proper record keeping, consistent filing, and regulatory compliance.	DOCUMENTATION	**Poor Records** Incomplete filings, missing paperwork, and inconsistent record-keeping
Visible Operations Open business activities, clear workflows, and verifiable processes.	OPERATIONAL TRANSPARENCY	**Complex/Secretive Workflows** Opaque business operations, unexplained transfers, and secretive acts.

Identifying behavioural red flags and suspicious transactional patterns

Illicit Financial Flows: Key Laundering Techniques

TACTIC 01 **Structuring / Smurfing**	Multiple cash deposits placed at diverse ATMs or branches consistently falling just below reporting limits (e.g., a narrow €9,000–€9,900 band).	Pattern & Threshold Analysis
TACTIC 02 **Money Mules / Funnel Accounts**	Rapid, high-frequency "pass-through" fund flows originating from geographically diverse accounts that consolidate into a single central node.	Network & Behavioural Modelling
TACTIC 03 **Trade-Based Money Laundering**	Significant price mismatches between invoiced values and known market prices, paired with shell companies trading in high-risk zones.	Cross-Referential Data Analytics
TACTIC 04 **Shell Corporation Layering**	Complex "U-turn" or "round-tripping" wire transfers across multiple offshore secrecy havens with vague generic invoice descriptions.	Transaction Path & Risk Scoring
TACTIC 05 **Cryptocurrency Obfuscation**	Transactions utilizing mixing services, tumblers, privacy-centric coins, or direct links to unverified wallets and darknet platforms.	Blockchain & On-Chain Heuristics

Regnology

Red Flags

based on AML/CFT authorities and standard-setting bodies

FATF + EU + US + UK

Customer-related

Transaction-related

Identifying behavioural red flags and suspicious transactional patterns

Identification & Behaviour

Red Flags

Customer-related

9 Critical Indicators

Grouped by sub-category: Disclosure · Profile · Conduct

01 Secretive or evasive

about identity, ownership, funds, or transaction purpose

02 Reluctant to provide

required information or documents

03 False or counterfeit

identification documents, or unverifiable

04 Unusual knowledge

of AML rules

05 Lifestyle inconsistent

lavish or inconsistent with known income

08 Reluctant to disclose parties

trusts, shell companies, or private investment companies

06 Criminal convictions

ongoing, or criminal connections

07 Adverse media

negative news about the client or associates

09 Has been refused services

or frequently changes advisors without clear reason

Identifying behavioural red flags and suspicious transactional patterns

Structure & Operations

Red Flags

Customer-related

5 Critical Indicators

Grouped by sub-category: Verifiability · Consistency · Risky Associations

01 Not easily verifiable

e.g. business entity not found on business register is publicly unavailable, outdated (jurisdiction with limited corporate transparency), + uses a non-professional email domain (e.g. Gmail, Yahoo)

02 No web presence

little to none, or phone numbers that do not match the expected country

03 Cannot or will not explain wealth

especially if inconsistent with income or business

04 Purposes not compatible

non-profit requesting services for purposes not compatible with its declared activities

05 Shares an address

with multiple companies, a sanctioned entity, or has a problematic / non-existent / residential address

Identifying behavioural red flags and suspicious transactional patterns

Transaction & Financial Activity

Red Flags

Transaction-related

7 Critical Indicators

Grouped by sub-category: Anomalous Patterns · Opacity · High-Risk Instruments

01 Unusual transactions

by size, nature, frequency, or manner of execution (e.g. cash on e-commerce, dormant accounts)

02 Large round amounts

or multiple small incoming transfers quickly wired abroad (preceded by a customer-details update)

03 Payment resubmission

repeated attempts to resend a rejected or blocked payment, often with slightly modified details

04 No legitimate purpose

no apparent legitimate business purpose, or overly complex for the stated reason

05 Multiple / foreign accounts

use of multiple bank accounts or foreign accounts without a good reason

06 Large private funding

bearer cheques or cash, especially if inconsistent with the client's profile

07 Document discrepancies

significant gaps between goods on the bill of lading, the invoice, and other documents

Identifying behavioural red flags and suspicious transactional patterns

Source of Funds & Geographical

Red Flags

Transaction-related

8 Critical Indicators

Grouped by sub-category: Source Legitimacy · Jurisdiction · Cross-Border Flow

01 No apparent connection

unusual source of funds, such as third-party funding with no legitimate explanation

02 Unjustified structures

shell companies or complex structures unjustified by the business profile

03 Private expenditure funded

by a company, business, or government

04 Illicit activity havens

countries with corruption, weak financial rules, or such reputations

05 Inadequate AML jurisdictions

client uses a VASP or foreign MVTS in weak-AML jurisdictions (frequent crypto-fiat / fiat-crypto)

06 Circumvention hubs

goods sent to, from, or through circumvention hubs or countries engaged with sanctioned states

07 Foreign with no link

funds move to / from foreign countries with no apparent client connection

08 High-risk country

parties native to, resident in, or incorporated in a high-risk country

Regnology

SESSION 2: Early Warning Indicators in Customer Due Diligence (CDD)

1 Methods of Enhanced Due Diligence (EDD) on high-risk customers

2 Identifying behavioural red flags and suspicious transactional patterns

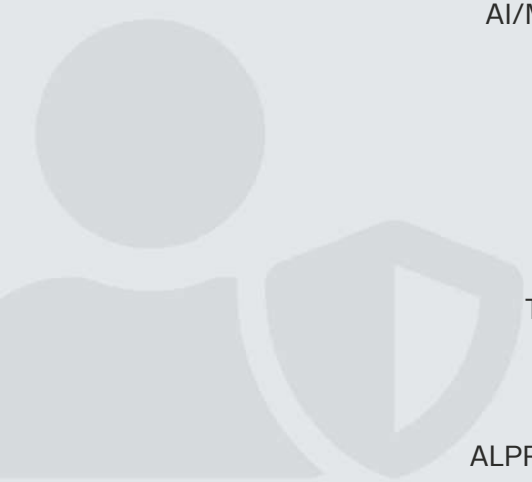
3 The role of technology in automating detection

The role of technology in automating detection

High-Stakes Technological Race

Technology is playing a **pivotal role** in the fight against organized crime, enabling law enforcement to analyse vast data and identify criminal activity. However, it is a **double-edged sword** — criminal organizations leverage the same advances to facilitate their illicit operations.

LAW ENFORCEMENT — DETECTION		ORGANISED CRIME — EVASION
Surveillance & analytics AI/ML detects patterns, predicts threats	VS	**Encrypted communication** Secure, anonymous coordination
Digital forensics Recovers data from seized devices		**Illicit markets** Dark web trafficking and data trade
Financial tracking Traces crypto via blockchain analysis		**Financial crime** Crypto laundering hides fund origins
Enhanced operations ALPR, facial recognition, response drones		**Advanced tech abuse** AI scams, deepfakes, smuggling drones



The role of technology in automating detection

The Shift from Manual to Automated Detection

These red flags **require a trained eye**, but **technology is becoming indispensable** for detecting the sophisticated methods used to obscure illicit actions.

MANUAL CDD · Traditional process

- Manual & time-consuming
- Prone to human error
- High volume of false positives
- Resource-intensive — high cost
- Struggles with transaction volume

AI

AUTOMATED AML · AI-based process

- Decreases errors
- Saves time and money
- More comprehensive risk coverage
- Real-time analysis
- Agile & scalable

CASE STUDY

Global Trust Bank cut fraud losses across all major categories with AI

Sources: Ademero – Global Trust Bank AI Fraud Detection Case Study (2024)

The role of technology in automating detection

Leveraging Technology: Automating Detection of Illicit Activities in CDD

The role of technology, particularly **AI and Machine Learning**, plays in automating the detection of indicators related to organized crime within the **Customer Due Diligence (CDD)** area:

1

Automation of Core CDD Processes

Customer identification & verification, screening against sanctions, and initial risk assessments — all automated.

- eID&V
- Sanctions Screening
- Risk Assessments

2

Automated Detection of Behavioural Red Flags

From static, rule-based systems to dynamic, behaviour-based monitoring. Baselines customer behaviour to surface red flags.

- Behaviour Monitoring
- Baseline Flags
- Rule → Dynamic

3

Improving Accuracy & Reducing False Positives

Shifts analysts from manual reviews to investigating the highest-risk alerts, significantly reducing false positives.

- High-Risk Alerts
- Fewer False Positives
- AI Prioritisation

4

Continuous Risk Assessment and Monitoring

Continuous & automated monitoring with real-time verification, keeping risk profiles up to date as new data arrives.

- Real-Time Monitoring
- Live Verification
- Real-Time Risk Profile

The role of technology in automating detection

How Technology Automates Detection: Key Technologies

Artificial Intelligence
& Machine Learning

Automation
RPA & onboarding

Biometrics
Identity & liveness

Blockchain & DLT
Crypto compliance

AI & ML — the role in crime detection

Role in detecting & disrupting crime

- Real-time risk assessment
- Monitor customer activity
- Build & update risk profiles
- Predictive analysis
- Anomaly detection
- Model criminal behaviour

Where AI is applied (survey of 88 pros)

- **82.5%** Transaction Monitoring
- **37.5%** Identity Verification
- **71.3%** AML
- **33.8%** Behaviour Analysis
- **61.3%** Anomaly Detection

Benefits: Faster detection 80% · Fewer false positives 73% · Better accuracy 61%

Automation — onboarding (CDD) & application areas

395 min
Manual onboarding / client

70 %
Less manual handling time

Tools: Robotic Process Automation · Real-Time Transaction Monitoring

Application areas

- **Risk Scoring** automated, updated
- **Data Gathering** collection & consolidation
- **Identity Verification** onboarding & verifying
- **Watchlist & Sanctions** PEPs, sanctions lists

Biometrics — KYC for AML compliance

- Synthetic-identity fraud — link physical self to digital ID in real time
- Liveness detection — skin-texture & action analysis beats deepfakes
- Real-time scoring — flag suspicion on the spot vs. laundering

Use cases:

- FinTech & Neobanks
- Crypto Exchanges
- E-commerce
- High-Value Finance

Blockchain & DLT — crypto compliance

Criminal use: ransom payments · darknet markets · terrorist financing · sanctions evasion · laundering networks

Public blockchains can be more traceable than cash through privacy coins and mixers complicate analysis.

Crypto-analytics tools:

ELLIPTIC · TRM · Chainalysis

Trace patterns & known wallets · de-mix Monero/tumblers via heuristics · FATF Rec.16 Travel Rule: VASPs share originator/beneficiary data

KYC360 / Nexus AML CDD Report (395 min, 70% reduction) | INFORM AI & Anti-FinCrime Survey 2026 (n=88)

The role of technology in automating detection

A View on the Risk the Technology Brings

Data Quality & Availability

AI performance hinges on data quality;

flawed data leads to unreliable results.

If AI trained on 2023 data it will not recognize 2024 patterns.

Algorithmic Bias

AI can learn and amplify societal biases from training data,

leading to discriminatory outcomes.

"Black Box" Transparency

Many advanced AI models

lack transparency, making their decision-making

hard to understand and challenging to hold accountable.

Adversarial Attacks

Criminals can deceive AI via adversarial attacks -

subtly manipulating data to cause the AI to make an error

Legal & Accountability Gaps

Lack of clear legal frameworks and accountability for AI errors

creates significant challenges for justice.

The role of technology in automating detection

Addressing the Risk the Technology Brings

Model Explainability & Decision Boundaries

GLOBAL System Logic

Why did you choose this specific model? How does the model weight risks?

Compliance document for the global logic of the system explanation.

LOCAL Specific Alerts

Why did this specific alert appear, and which characteristics triggered it?

E.g., 400% increase in cross-border velocity; connection to a sanctioned jurisdiction from a third party.

COUNTERFACTUAL Stress-Test

What would have to be changed for this customer NOT to be flagged?

Reveals decision boundaries and sensitive parameter paths.

Machine-Generated Alert → Human-Led Defensible Decision

ALERT SCENARIO (ANOMALY DETECTED)

A vessel turned off its navigation device and later investigation showed it was not a technical issue — and it happened in a high-risk corridor.

Machine provided a raw red flag indicating suspicious activity.

HUMAN RESOLUTION (DEFENSIBLE DECISION)

Machine provided a red flag, but it needed to be justified and verified for the SAR (Suspicious Activity Report).

Expert contextualizes the signal into an auditable regulatory outcome.

Regnology

Session 3: Supply Chain Vulnerabilities and Due Diligence

1 Mapping and assessing risks within the supply chain | 2 Red flags in supply chain management | 3 Best practices for supply chain transparency and continuous monitoring.

Regnology

Session 3: Supply Chain Vulnerabilities and Due Diligence

1 Mapping and assessing risks within the supply chain|

2 Red flags in supply chain management|

3 Best practices for supply chain transparency and continuous monitoring.

Mapping and assessing risks within the supply chain

Mapping Risk Across the Tiers

As you move deeper into the chain, visibility falls but laundering risk rises. The payments layer cuts across every tier.

TIER 1

Direct Supplier / Customer

Visibility: HIGH
ML risk: managed

CDD / KYC / EDD applied directly
You onboard and screen this party yourself.

TIER 2

Supplier's Supplier

Visibility: LIMITED
ML risk: rising

Reached only via KYS / supplier DD
Indirect — standard CDD does not see this far.

TIER 3+

Deep / Hidden Nodes

Visibility: LOW / NONE
ML risk: highest

Network & trade-document analysis
Where shells, diversion and TBML concentrate.

Cross-cutting payments layer (TBML): money laundering and fake invoicing flow through **every tier** — independent of where the goods physically are.

The deeper the tier, the lower the visibility and the higher the residual ML risk — see next slide for scoring.

Mapping and assessing risks within the supply chain

Managing Risk Across the Tiers

What is SCRM and Why It Matters

Understanding the fundamentals of supply chain risk management and its strategic importance

Definition

What SCRM means

Supply Chain Risk Management (SCRM) is the systematic identification, assessment, mitigation, and monitoring of risks across the end-to-end supply chain.

- **End-to-end visibility**
  Monitor suppliers, logistics, and distribution channels
- **Proactive risk mitigation**
  Prevent disruptions before they occur
- **Continuous monitoring**
  Real-time tracking of risk indicators

ISO 31000 Compliant Secure Framework

Why It Matters

Strategic benefits

Resilience
Build business continuity

Cost Reduction
Reduce disruption costs

Reputation
Protect brand image

Compliance
Ensure regulatory adherence

Mapping and assessing risks within the supply chain

Supply Chain Risk Process

1 Identify
Risk Discovery

- **Map tiers & dependencies**
  Analyse supplier network
- **Collect data**
  Internal & third-party
- **Threat vectors**
  Identify vulnerabilities

Status: Active

2 Assess
Risk Analysis

- **Evaluate likelihood**
  Probability assessment
- **Impact analysis**
  Consequence evaluation
- **Prioritize risks**
  Risk scoring

Status: In Progress

3 Mitigate
Risk Treatment

- **Define controls**
  Risk treatments
- **Assign owners**
  Responsibility
- **Set timelines**
  Implementation

Status: Pending

4 Monitor
Continuous Oversight

- **Track KPIs**
  Performance metrics
- **Audit regularly**
  Compliance checks
- **Refine plans**
  Update strategies

Status: Ongoing

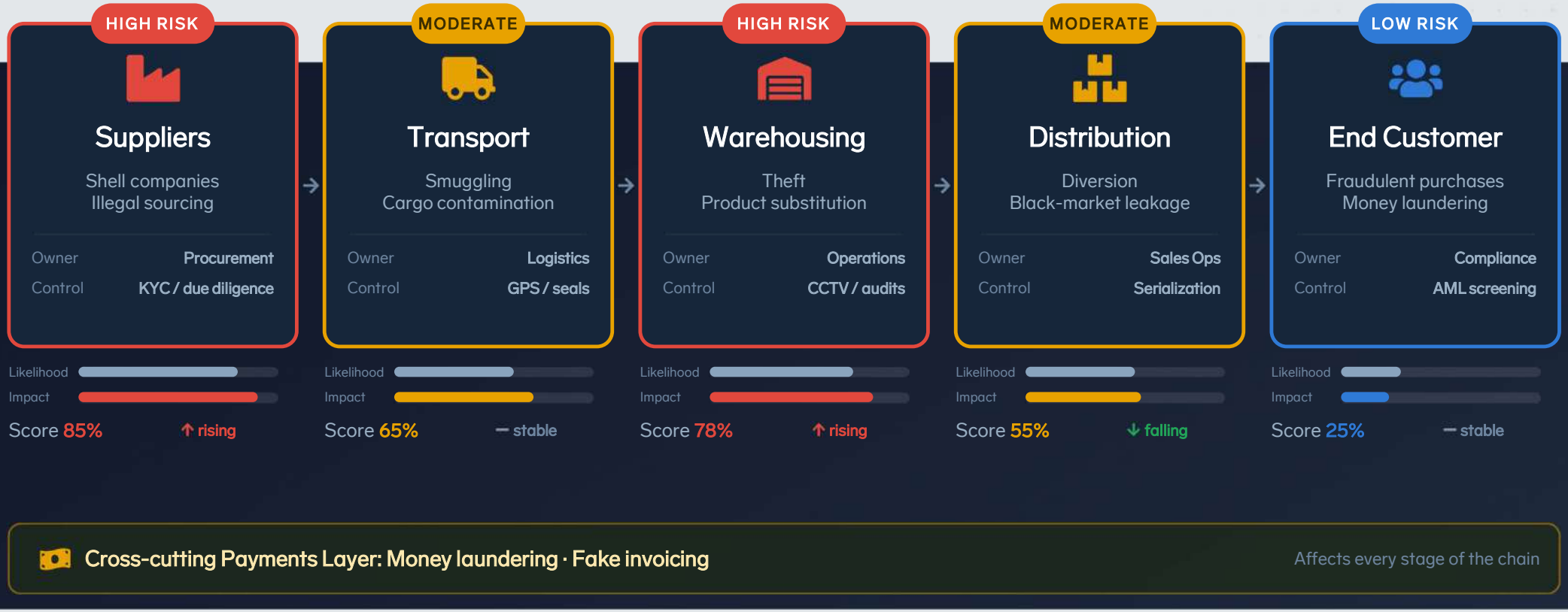
Identify → Assess · Assess → Mitigate · Mitigate → Monitor · Monitor → Identify

Continuous cycle

ISO 31000 Compliant · Secure Framework

Mapping and assessing risks within the supply chain

Supply Chain Risk Mapping



Critical Risk (75–100%) Moderate Risk (50–74%) Low Risk (0–49%)

Risk score = Likelihood × Impact

Mapping and assessing risks within the supply chain

AML Beyond Tier 1

TIER 1 — DIRECT CUSTOMER / SUPPLIER

Covered by the AML section: CDD, KYC, EDD, PEP & UBO checks on the entity you onboard directly.

TIER 2 / TIER 3 — DEEPER IN THE CHAIN

Supplier's suppliers — invisible to standard CDD. This is where laundering risk re-emerges and must be addressed separately.

BRIDGE 1

Trade-Based Money Laundering (TBML)

Laundering moves through trade and invoices, not just wire transfers — so it flows across every tier of the chain.

- Over- / under-invoicing, false invoicing, shell companies
- Mismatch between goods, value and shipment documents
- = the cross-cutting payments layer from the Mapping slide

Source: FATF/Egmont, Trade-Based Money Laundering — Trends & Developments (2020); TBML Risk Indicators (2021).

BRIDGE 2

Supplier / Third-Party Due Diligence (KYS)

The same AML toolkit — extended from the customer to suppliers, including deeper tiers.

- Risk-based: EDD for high-risk suppliers, SDD for low-risk
- Triggers: FATF grey-list location, cash-intensive sector, PEP in UBO
- "Know Your Supplier" (KYS) = KYC applied across tiers

Source: industry AML practice — Third-Party / Supply-Chain ML risk (TPDD / KYS).

SCRM asks: will the delivery arrive? **AML asks:** is this flow clean?.

Mapping and assessing risks within the supply chain

Supply Chain Risk Classification

Known Internal
Process & Quality

Low Risk

- **Process Failures** — High
  Manufacturing yield, receivables, payables
- **Quality Issues** — Medium
  QA/QC failures, defects, returns
- **Capacity Constraints** — Low
  Equipment, labour, resources

Mitigation: 85%

Known External
Supplier & Market

Medium Risk

- **Supplier Bankruptcy** — High
  Financial stability, credit risk
- **Geopolitical Events** — Medium
  Trade wars, sanctions, conflicts
- **Market Volatility** — Medium
  Price fluctuations, demand changes

Mitigation: 65%

Unknown Internal
Latent Weaknesses

Medium Risk

- **Undiscovered Vulnerabilities** — High
  Hidden process flaws, system gaps
- **Latent Weaknesses** — Medium
  Unidentified capacity issues
- **System Gaps** — Low
  Undetected control failures

Mitigation: 45%

Unknown External
Black Swan Events

High Risk

- **Black Swan Events** — Critical
  Unforeseen disruptions
- **Natural Disasters** — High
  Earthquakes, floods, volcanoes
- **Market Shocks** — High
  Sudden economic changes

Mitigation: 25%

Knowledge Types
Risk awareness levels

- **Known Knowns** — 85%
  Risks we know about and can quantify
- **Known Unknowns** — 65%
  Risks we know exist but can't measure
- **Unknown Unknowns** — 25%
  Risks we don't know exist
- **Unknown Knowns** — 15%
  Risks we're ignoring

Key Insight:

Organizations should focus on converting "known unknowns" to "known knowns" through better data collection and analysis.

Mapping and assessing risks within the supply chain

Supply Chain Risk Types

Operational
High

Process failures, capacity constraints

Key areas: Process gaps enabling TBML, weak documentation, inconsistent invoices, poor trade controls.

Impact: High

Financial
Medium

Cost volatility, credit issues

Key areas: Payment structuring, rapid movement of funds, threshold activity, crypto exposure, unusual wire patterns.

Impact: Medium

Geopolitical
High

Trade restrictions, sanctions

Key areas: High-risk jurisdictions, sanctions exposure, FATF grey/black list, trade route risk.

Impact: High

Environmental
Medium

Climate events, disasters

Key areas: Disruptions causing rushed routing, abnormal shipment changes, emergency re-routing (OC opportunity)

Impact: Medium

Cybersecurity
High

Data breaches, attacks

Key areas: Ransomware, malware, hacking with redirecting payments, stealing profiles for deep fakes

Impact: High

Supply
Medium

Shortages, delays

Key areas: Tier 2+ blind spots, shell companies, complex ownership, limited beneficial ownership visibility

Impact: Medium

Demand
Low

Forecast errors, spikes

Key areas: Forecasting, market shifts, negative ML-related media

Impact: Low

Total Risks

7 categories

7

Active monitoring

Mapping and assessing risks within the supply chain

Supply Chain Risk Examples

Single Point of Failure

One supplier, plant, or chokepoint halts the whole chain.

• **Real case** Suez Canal, 2021: the Ever Given blocked the canal for 6 days, holding up ~$9 bn of trade per day and forcing 400+ ships to wait or reroute around Africa.

Lack of Visibility

Firms know Tier-1 suppliers, rarely Tier-2 and Tier-3 — risk hides deep in the chain.

• **Real case** Goldex Case (Colombia): Illegal gold mixed into legitimate exports through over-invoicing. Contaminated global gold supply chain (refineries → electronics & jewelry). Highlighted weak supplier due diligence and traceability.

Geographic Concentration

Production clustered in one region multiplies exposure to disasters, sanctions and tensions.

• **Real case** COVID-19 lockdowns in Malaysia & SE Asia (2021) exposed over-reliance on single regions, deepening the global chip crisis.

Lean / Just-in-Time

Minimal stock means no buffer — the smallest delay cascades across the chain.

• **Real case** Chip shortage, 2021: thin buffers cost the auto industry ~$210 bn in revenue and ~11 m fewer vehicles built.

Cyber & IT Dependency

An attack on one node — a software supplier — paralyzes many downstream firms at once.

• **Real case** Ransomware on a single logistics or software vendor can freeze operations across every customer that depends on it.

Black-Swan Shocks

Disasters, wars, sanctions, sudden economic shocks — unpredictable by nature, hardest to hedge.

• **Real case** Russia's airspace closure (2022) cut air-freight alternatives overnight, showing how fast a single mode can vanish.

Mapping and assessing risks within the supply chain

Supply Chain Risk Mitigation

Not every supply-chain control affects laundering risk the same way. Some lower AML exposure, some are neutral, and some raise it.

↓ Lowers AML exposure — Neutral for AML ↑ Raises AML exposure

↓ LOWERS AML EXPOSURE

Supplier mapping & tier visibility

Seeing Tier 2/3 removes the CDD blind spot.

Supplier onboarding / KYC + audits

Same checks catch opaque UBO & invoice anomalies.

— NEUTRAL FOR AML

Safety stock & capacity buffers

Improves continuity — no effect on laundering risk.

Logistics / route optimization

Operational only, unless routed via a high-risk hub.

↑ RAISES AML EXPOSURE

Diversifying into weak-AML jurisdictions

Resilience gain, but new grey-list exposure.

Adding many new / unvetted suppliers

More nodes = more laundering entry points.

IT SYSTEMS IN SCRM — the strongest lever on AML exposure

ERP / supplier platforms, e-invoicing and shared data **lower** AML exposure — they make invoices, ownership and flows auditable, and feed screening, trade-document checks and network analysis across tiers. **But** fragmented, siloed or poorly integrated systems **raise** it — blind spots and unreconciled data are exactly where TBML hides.

Analytical view — map each SCRM control against AML risk before assuming a win-win. Overlap is real, but so are trade-offs.

Mapping and assessing risks within the supply chain

Black Swan Events – Potential AML Gateway

A sudden **shock** forces fast supply-chain **changes**. When new solutions outpace **controls**, they open a **window** for money laundering.

1

The Shock

Disruption forces new suppliers, new lines and emergency procurement — all under time pressure.

2

Rushed Fixes

Onboarding & due diligence simplified, controls relaxed, oversight deferred to keep goods flowing.

3

Window Opens

Criminals deliberately bypass weakened DD, exploit emergency funds and cash-intensive lines.

4

Residual Exposure

Disorderly supplier shutdowns and unvetted nodes leave lasting ML/TF vulnerabilities.

THE MITIGANT — relax deliberately, not chaotically

Keep a **risk-based approach even under pressure:** simplify only where risk is genuinely lower, re-screen every new / emergency supplier, restore deferred oversight fast, and keep filing suspicious reports. FATF permits flexibility — but **deliberately, never as a blanket drop in controls.**

9/11 Attacks (2001) | Global Financial Crisis (2008) | Bitcoin & Crypto (2009+) | COVID-19 (2020) | Russia–Ukraine War (2022)

Mapping and assessing risks within the supply chain

Supply Chain Risk Toolkit

Two layers, one system. The **risk-management process** defines what to do about a risk; the **toolkit** makes it visible and executable.

Risk-Management Process

SCRM · the method — tool-independent

1 Spot & Forecast
Identify exposures, predict where disruption may hit

2 Assess & Warn
Score likelihood × impact; issue prioritized warnings

3 Respond & Recover
Mitigate, reroute, activate contingency plans

The Toolkit

Implementation — what the user sees

A Monitoring & Alert Systems
Real-time anomaly detection — feeds the Spot step

B Risk Scoring & Visualization
Dashboards and maps that rank the Assess step

C Response & Routing Tools
Playbooks & routing engines for the Respond step

PROCESS ↔ TOOLKIT

two halves of one system

Regnology

Session 3: Supply Chain Vulnerabilities and Due Diligence

1 Mapping and assessing risks within the supply chain |

2 Red flags in supply chain management |

3 Best practices for supply chain transparency and continuous monitoring.

Red flags in supply chain management

Key Weak Points in Modern Supply Chains

Vulnerability	Description	Risk Level
🗂️ **Complexity**	Numerous intermediaries and touchpoints — the root of the two traits below.	High
└ 🔗 Interdependence	Tightly linked nodes mean one disruption cascades across the whole chain.	High
└ 👁️ Limited Visibility	Firms know Tier-1 suppliers, rarely Tier-2/3 — risk hides deep in the chain.	High
🌐 **Globalization**	Root driver — operating worldwide spawns the three traits below.	High
└ 🧭 Geographic Dispersion	Physical sites spread across regions exposed to local disasters and instability.	High
└ ⚖️ Multiple Jurisdictions	Many legal and regulatory systems create disparities and exploitable loopholes.	High
└ 🤝 Outsourcing	Third parties run operations — dependence on their standards and integrity.	Medium
💎 High-Value Goods	The sheer volume and value of transported goods attract theft.	Medium
💻 Digitalization	Heavy reliance on digital systems exposes networks to cyber threats.	Critical
🏛️ Insider Threats	Complicit or coerced employees present significant internal risks.	Critical

Red flags in supply chain management

Supply Chains Vulnerability Areas

Structural & Operational

Physical infrastructure risks

Complexity & Transparency

Complex supply chains create "blind spots" for illicit goods

FTZ Abuse

Reduced oversight enables concealment

Postal Exploitation

High volume prevents inspection

Digital

Technology-based risks

Online Anonymity

E-commerce anonymity hampers prosecution

Document Falsification

Forged documents disguise illicit goods

Regulatory & Human

Governance and control issues

Corruption

Officials enable illegal shipments

Insufficient Controls

Lack of resources for monitoring

Organised Crime Favourable Conditions

Key factors enabling criminal activity in supply chains

- **Patchy Legal Frameworks** — Inconsistent regulations
- **Low Prosecution Priority** — Minimal enforcement
- **Little Deterrent Penalties** — Weak consequences

Red flags in supply chain management

Red Flag Category: Business & Transactions

Opaque / Shell Structures

Complex ownership or P.O.-box vendors with no clear business justification.

Unusual Payment Patterns

Sudden volume spikes to one vendor, or multiple invoices on the same day.

Outside Normal Systems

Manual payment approvals or clearing payments without proof of delivery.

Abnormal Vendor Selection

One person solely choosing key suppliers — a sign of possible collusion.

Anomalous Pricing

Paying well above market rates, often masking kickbacks or illicit payments.

Limited Access During Audits

Restricted access to warehouses or production lines during audits.

Red flags in supply chain management

Red Flag Category: Logistics & Transportation

EGMONT GROUP OF FINANCIAL INTELLIGENCE UNITS

EUROPOL

EU-SOCTA
EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

FATF

Inconsistent Routing

Shipping routes that defy geographical or economic logic.

"Circumvention Hubs"

Goods transiting through countries known for weak export controls or sanctions evasion.

Information Reluctance

Refusal to disclose the final destination or end-user of the cargo.

Compromised Integrity

Tampered container seals or the discovery of unauthorized GPS trackers.

Insecure Practices

Routine use of unsecured parking or deviations from planned secure routes.

Multiple Shipments

Repeated shipments of identical goods over a short period without clear economic justification.

Abuse of Free Trade Zones

Misuse of free trade zones (FTZs) as a key indicator of potential Trade-Based Money Laundering (TBML).

Red flags in supply chain management

Red Flag Category: Digital & Cyber Threats

Targeted Phishing & Malware

Attempts to steal credentials for cargo-management systems.

Fraudulent Digital Profiles

Fake carrier profiles on freight platforms.

Ransomware Attacks

Data encryption to disrupt operations and cover tracks.

Anonymizing Technologies

Crypto or mixers to obscure illicit vendor payments.

Compromised Vendor Access

Anomalous lateral movement or unusual data access via a vendor.

EUROPOL
EU-SOCTA
EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

BIGS
BRANDENBURGISCHES INSTITUT für GESELLSCHAFT und SICHERHEIT

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA

verizon business
2025 Data Breach Investigations REPORT

Red flags in supply chain management

Red Flag Category: Employee & Insider Threats

EUROPOL

EU-SOCTA
EUROPEAN UNION SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT

Unexplained Lifestyle Changes

Sudden wealth that doesn't match an employee's salary or position.

Colleague Tips

Coworker reports of anomalous behaviour, secrecy, or skipped procedures.

Lack of Hiring Due Diligence

Skipping background checks for sensitive logistics or financial roles.

High Turnover in Key Roles

Instability in critical positions - a precursor to infiltration.

Unusual Access / Hours

Logins at odd hours or while on leave; access beyond role.

Reluctance to Take Leave

Avoiding handover that could expose a hidden scheme.

Red flags in supply chain management

Proactive Mitigation Framework

Enhanced Due Diligence

Deep-dive background checks on partners, suppliers, and key employees.

Advanced Technology

Deploy AI-powered anomaly detection and real-time track-and-trace platforms.

Intelligence Sharing

Collaborate with industry peers, law enforcement, and regulatory bodies.

Comprehensive Training

Empower staff across all levels to recognize and safely report red flags.

Physical Security

Audit and strictly upgrade access controls at warehouses, ports, and hubs.

Unified Defence

Regnology

Session 3: Supply Chain Vulnerabilities and Due Diligence

1 Mapping and assessing risks within the supply chain | 2 Red flags in supply chain management |

3 Best practices for supply chain transparency and continuous monitoring.

Best practices for supply chain transparency and continuous monitoring

What is Supply Chain Transparency?

MIT Center for Transportation & Logistics

Alexis Bateman, director of MIT Sustainable Supply Chains, says transparency consists of two core elements:

Visibility

Accurately identifying and collecting data from all links in your supply chain.

Disclosure

Communicating that information internally and externally at the level of detail required or desired.

Related, but Distinct

Traceability

Ability to follow materials/products through the the chain and verify provenance.

Visibility

Access to timely, accurate multi-tier data for internal control and risk.

Transparency

Intentional disclosure of selected data to stakeholders (beyond minimum compliance).

Best practices for supply chain transparency and continuous monitoring

Why is it Important?

- Ensures operations are ethical, sustainable, and reliable.
- Majority of consumers demand to know where their products come from.
- Builds vital trust with consumers and investors.
- Fulfils growing regulatory mandates like the EU's CSRD.

Key Drivers

Regulatory Pressure

Consumer & Investor Trust

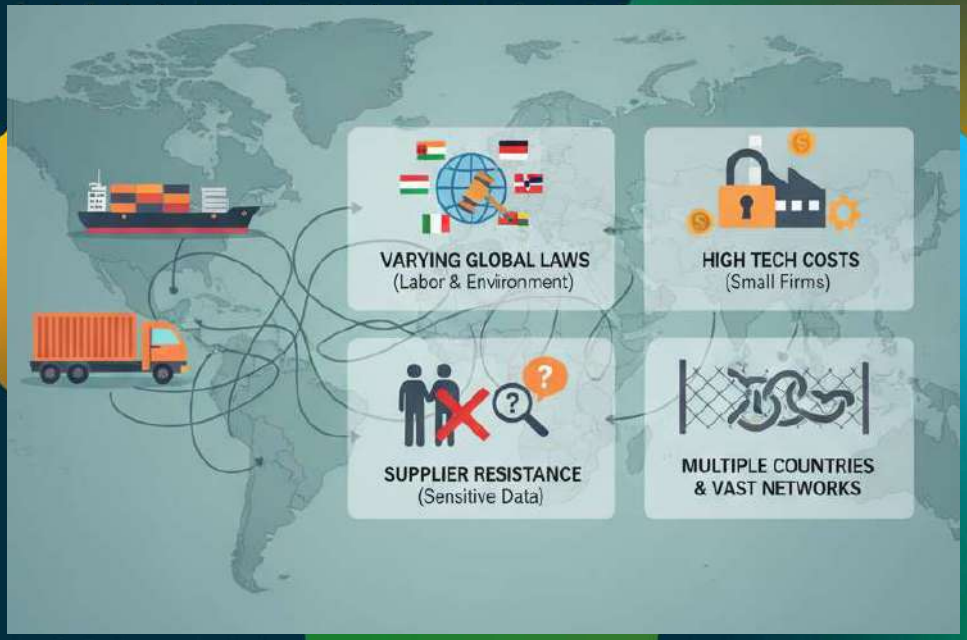
Risk Mitigation

ESG & Impact Investing

Best practices for supply chain transparency and continuous monitoring

Key Challenges within the Supply Chain Transparency and Continuous Monitoring

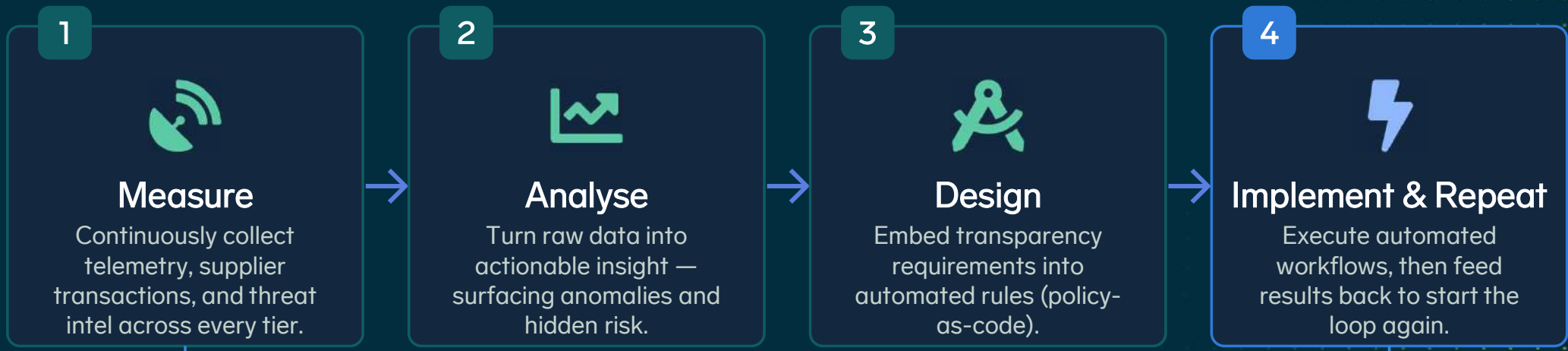
- Modern supply chains span multiple countries and vast networks.
- Varying global laws regarding labour and environmental practices.
- High costs of implementing required technology for smaller firms.
- Potential resistance from suppliers to share sensitive data.



Best practices for supply chain transparency and continuous monitoring

Continuous Monitoring Lifecycle

Continuous monitoring **replaces outdated periodic reviews** with proactive real-time assessments.



↺ Continuous feedback loop — results from Implement flow back into Measure, so the chain is never "reviewed once and forgotten."

Best practices for supply chain transparency and continuous monitoring

Supply Chain Transparency: Best Practices (Part 1)

Foundation — Map & Standardize

Supply Chain Mapping

Document every supplier, site, and logistics partner. Visualizing the value chain reveals location and concentration risks.

Establish Clear Standards

Define and communicate standards for quality and ethical sourcing. Track compliance with KPIs.

Align with Recognized Standards

Adopt frameworks like ISO 20400 and map beyond Tier 1 into Tier 2-3, where hidden risk concentrates.

Best practices for supply chain transparency and continuous monitoring

Supply Chain Transparency: Best Practices (Part 2)

Verify & Capture Data

Verification & Audits

Conduct regular verifications: on-site inspections, document reviews, and independent third-party audits.

- On-site inspection
- Document review
- 3rd-party audit

Data Collection & Sharing

Consolidate transaction and performance data of trading partners. Verify supplier data continuously.

Partner data verified

Leverage Technology

Embrace modern tools — blockchain, RFID, AI, and IoT — for accuracy and real-time visibility.

Blockchain | RFID | AI | IoT

Best practices for supply chain transparency and continuous monitoring

Supply Chain Transparency: Best Practices (Part 3)

People & Communication

Foster Collaboration

Build open, mutually beneficial relationships with all suppliers. Transparency is built together, not imposed.

Communicate Transparently

Openly share supply chain challenges, goals, and ongoing progress with all relevant stakeholders.

Suppliers Customers Regulators Public

Share openly with all stakeholders

Engage & Train Suppliers

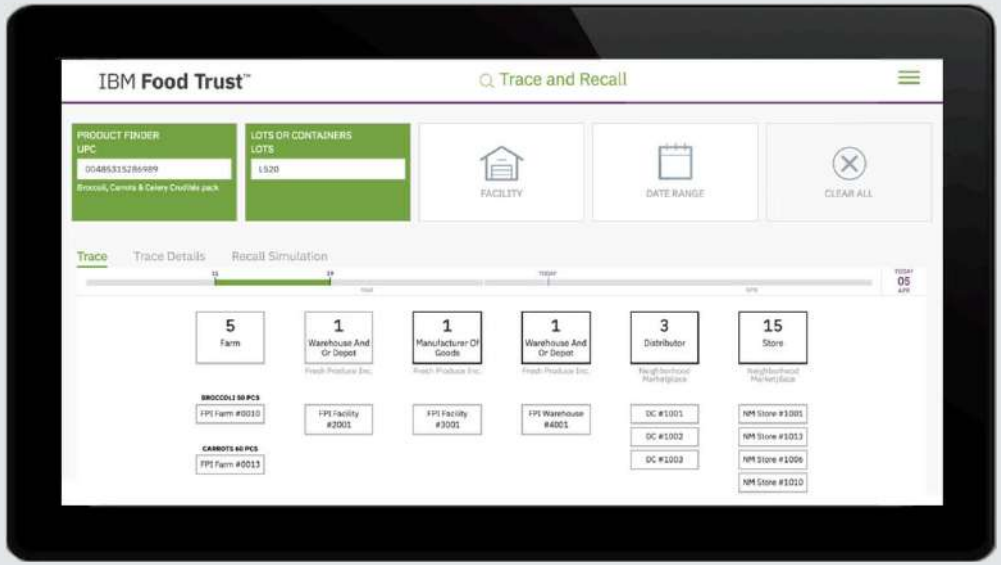
Support suppliers with training, capacity-building, and incentives to meet transparency requirements.

Train → Build capacity → Incentivize

Best practices for supply chain transparency and continuous monitoring

Supply Chain Transparency: **Real-World Examples**

- IBM® Food Trust is a software-as-a-service (SaaS) food-safety solution
- Enables a network of participants across the food supply chain to collaborate and securely share data



IBM

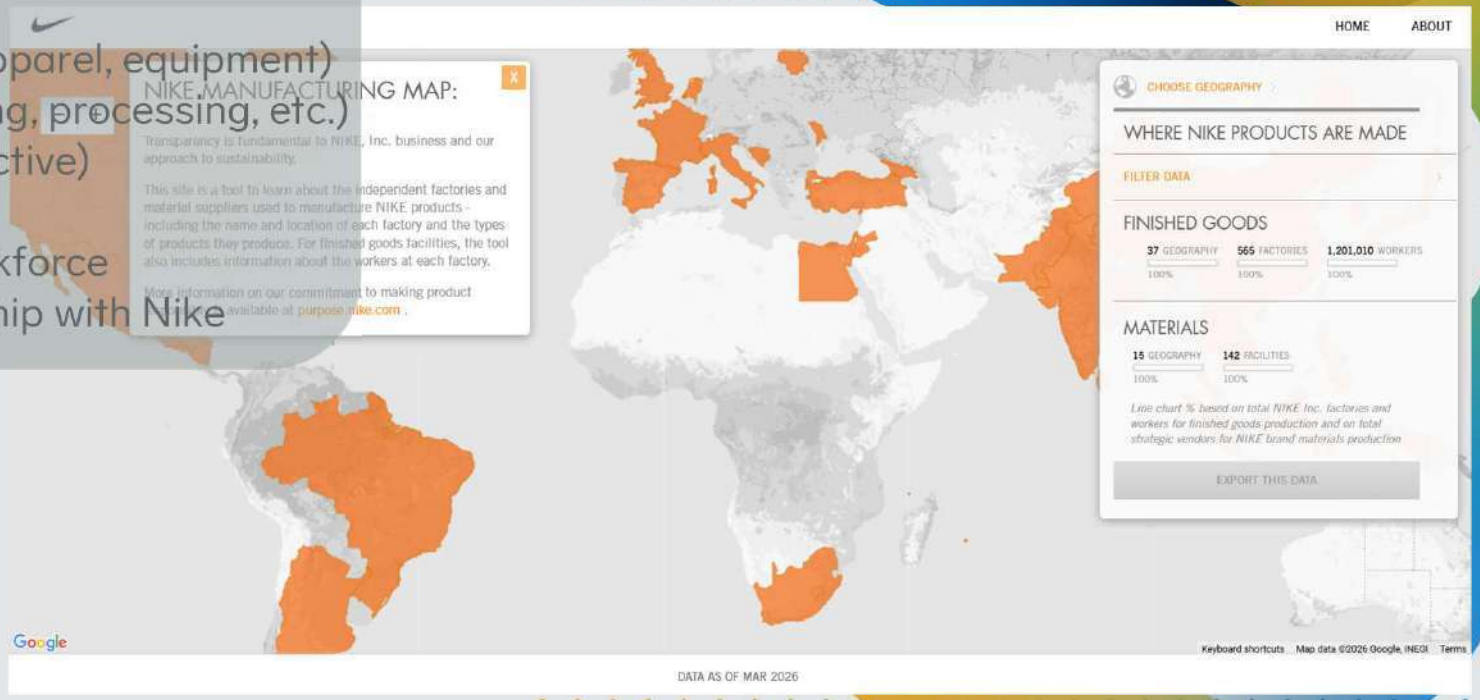
Walmart

Best practices for supply chain transparency and continuous monitoring

Supply Chain Transparency: Real-World Examples

Data shown on the Nike Manufacturing Map

- Supplier/factory name
- Location (country, city)
- Address
- Product type (footwear, apparel, equipment)
- Facility type (manufacturing, processing, etc.)
- Factory status (active/inactive)
- Workforce size (range)
- Gender breakdown of workforce
- Start date of the relationship with Nike



Thank You

Regnology

data | cros 3

Co-funded by the European Union

DATACROS III

Developing an Ethical AI-driven Tool-box for Boosting Cross-border Financial Investigations on Organised Crime Networks

THE DATACROS III TOOLBOX

Michael Lo Giudice
Michaelvictor.logiudice@unicatt.it

data | cros 3

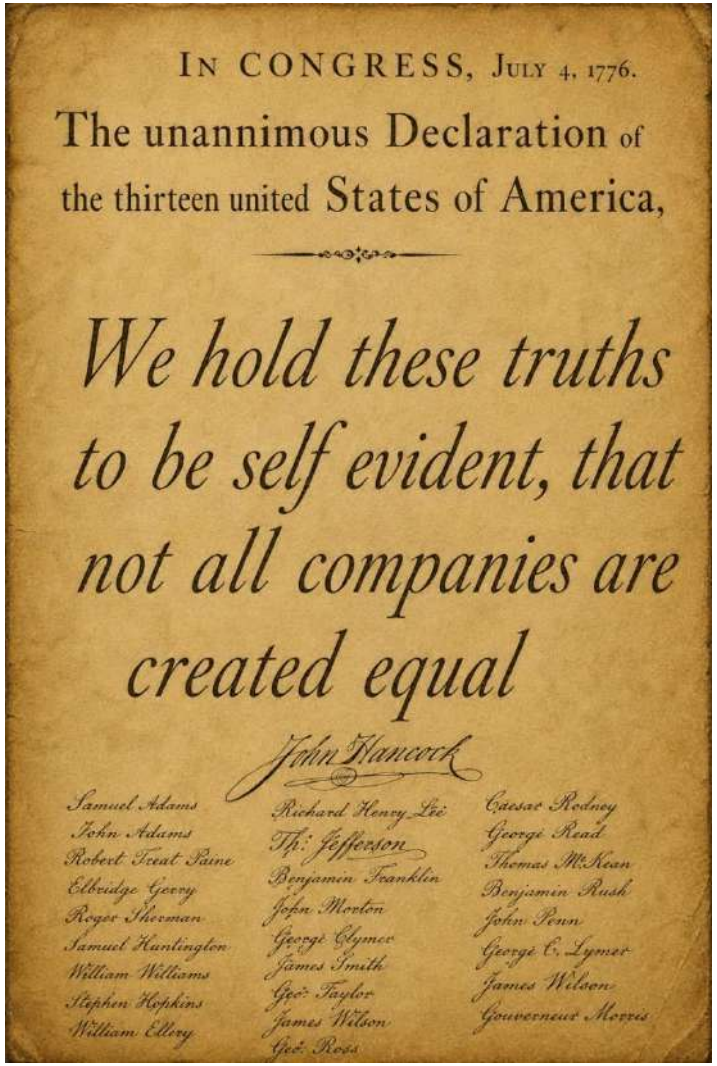
TRANSCRIME

UNIVERSITÀ CATTOLICA del Sacro Cuore

Regnology

SYNTHETIC RISK INDICATORS

SYNTHETIC RISK INDICATORS


IN CONGRESS, JULY 4, 1776.

The unanimous Declaration of the thirteen united States of America,

We hold these truths to be self evident, that not all companies are created equal

John Hancock

Samuel Adams
John Adams
Robert Treat Paine
Elbridge Gerry
Roger Sherman
Samuel Huntington
William Williams
Stephen Hopkins
William Ellery

Richard Henry Lee
Th: Jefferson
Benjamin Franklin
John Morton
George Clymer
James Smith
Geo: Taylor
James Wilson
Geo: Ross

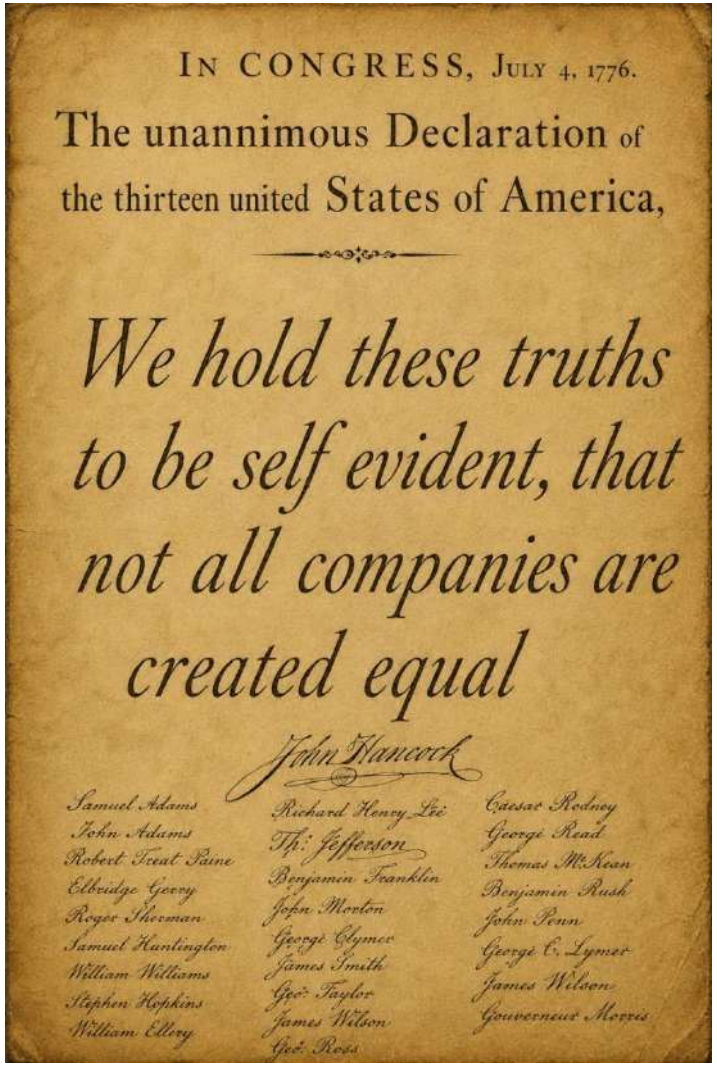
Caesar Rodney
George Read
Thomas M'Kean
Benjamin Rush
John Penn
George C. Lymer
James Wilson
Gouverneur Morris

Corporate Risk Indicators:

- Scoring and red-flag detection applied to the characteristics of corporations
- Based on the study of previous entities used in financial and organised crime – as well as cases of corruption

THE OWNERSHIP MONITOR

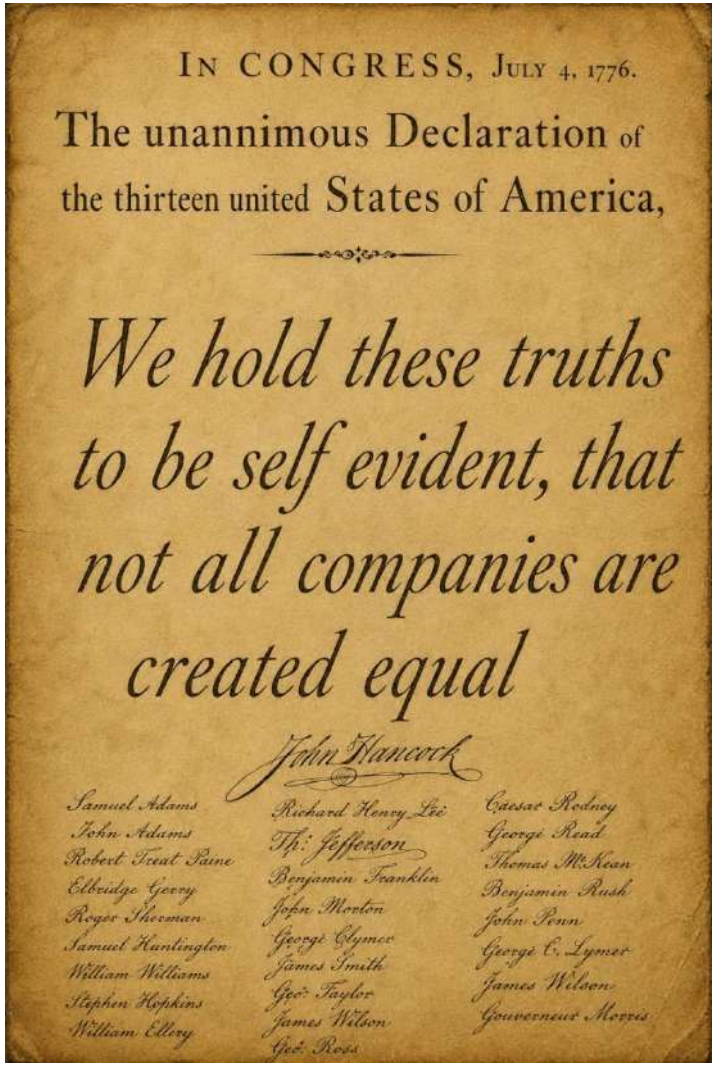
SYNTHETIC RISK INDICATORS



Corporate Risk Indicators:

- Scoring and red-flag detection applied to the characteristics of corporations
- Based on the study of previous entities used in financial and organised crime – as well as cases of corruption

SYNTHETIC RISK INDICATORS



Corporate Risk Indicators:

- Scoring and red-flag detection applied to the characteristics of corporations
- Based on the study of previous entities used in financial and organised crime – as well as cases of corruption

SYNTHETIC RISK INDICATORS

	A	B	C	D	E	F	G
1							
2		**Apple Inc. Balance Sheet**					
3		($ in millions)				**2020A**	**2021A**
4							
5		Cash and Cash Equivalents				$191,830	$190,516
6		Accounts Receivable, net				16,120	26,278
7		Inventories				4,061	6,580
8		Other Current Assets				32,589	39,339
9		**Total Current Assets**				**$244,600**	**$262,713**
10							
11		Property, Plant and Equipment, net					440
12		Other Non-Current Assets				42,522	
13		**Total Assets**				**$323,888**	**$351,**
14							
15		Accounts Payable				$42,296	54,76
16		Other Current Liabilities				42,684	493
17		Commercial Paper				4,996	6,00
18		Deferred Revenue				6,643	7,61
19		**Total Current Liabilities**				**$96,619**	**$115,8**
20							
21		Long-Term Debt				$107,440	$1
22		Other Non-Current Liabilities				54,490	
23		**Total Liabilities**					**$287,9**
24							
25		Common Stock and APIC				$50,779	$57,365
26		Retained Earnings				14,966	5,562
27		Other Comprehensive Income / (Loss)				(406)	163
28		**Total Shareholders' Equity**				**$65,339**	**$63,090**
29							
30		*Check*				--	--

SYNTHETIC RISK INDICATORS

TERR

COM
HIST

CORP
STRU

CONNECTIONS

› Flags when BOs/directors are:
  - Political exposed persons
  - Public office holders
› Public Tender Participation
› s publication features
el risk
ts
sanctioned subjects
financial penalites
re leaks & adverse media
exchanges
rs that

› High n° of
insolvent,
› Shares leg
› Shares leg
insolvent,

(compared to the firm's legal address)

ELSEVIER
Journal of Economic Criminology
Volume 10, December 2025, 100184

Home › Trends in Organized Crime › Article

***Ville lumière Ou Ville obscure?* Assessing the secrecy of firms owning real estate properties in Paris**

Research Article

Financial crime risk assessment: machine learning insights into ownership structures in secr

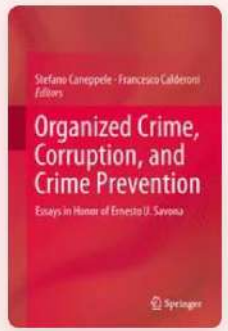
Home › Organized Crime, Corruption and Crime Prevention › Chapter

When Criminals Invest in Businesses: Are We Looking in the Right Direction? An Exploratory Analysis of Companies Controlled by Mafias

Chapter | First Online: 31 October 2013

pp 197–206 | Cite this chapter

Save chapter



Organized Crime, Corruption and Crime Prevention

DATACROS III WORKFLOW

RESEARCH

TRANSCRIME
Joint Research Centre on Innovation and Crime

Crystal

Government Transparency Institute

CERTH

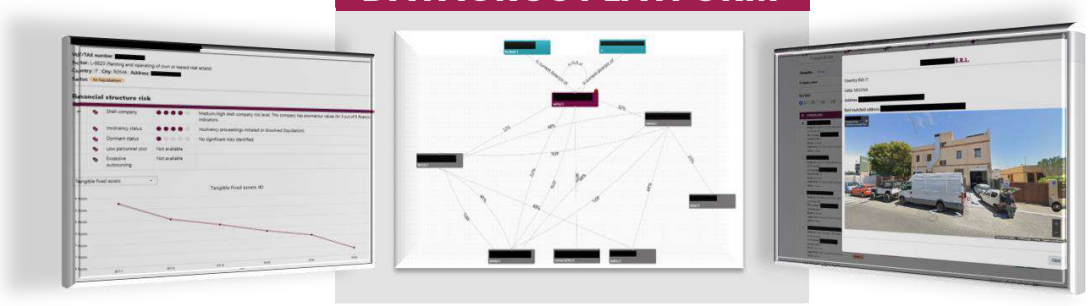
Regnology

RESEARCH FINDINGS

TECHNICAL DEVELOPMENT

RISK INDICATORS & AI-TECHNOLOGY

DATACROS PLATFORM



INPUT & KNOW-HOW

LEA EXPERTS

ANABI
SCO
Financial Intelligence Unit
Autorité de la concurrence
ÚOHS
ANAC
NTA

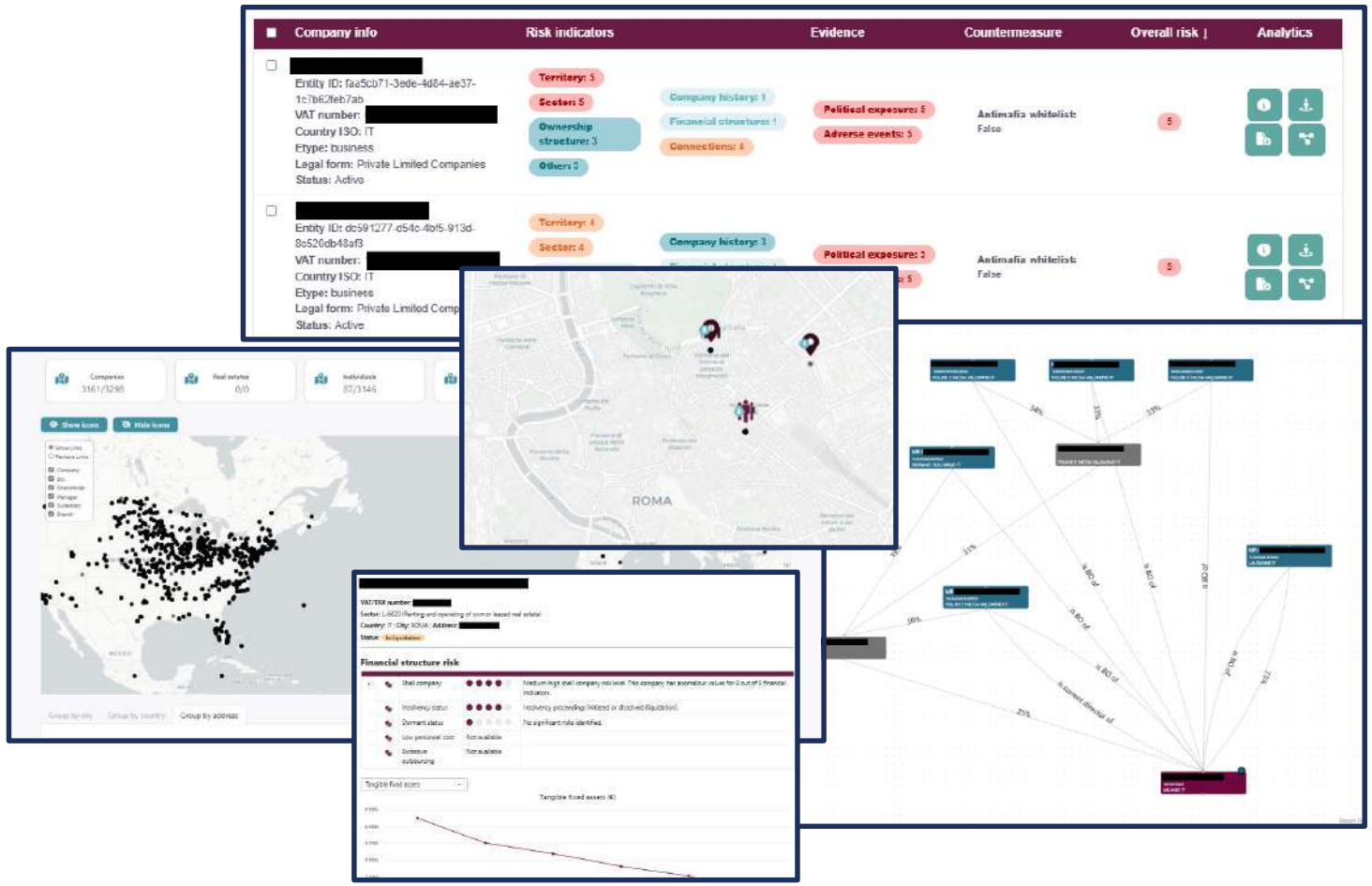
INVESTIGATIVE JOURNALISTS

context
OCCRP
IRPI MEDIA

VALIDATION & FEEDBACK

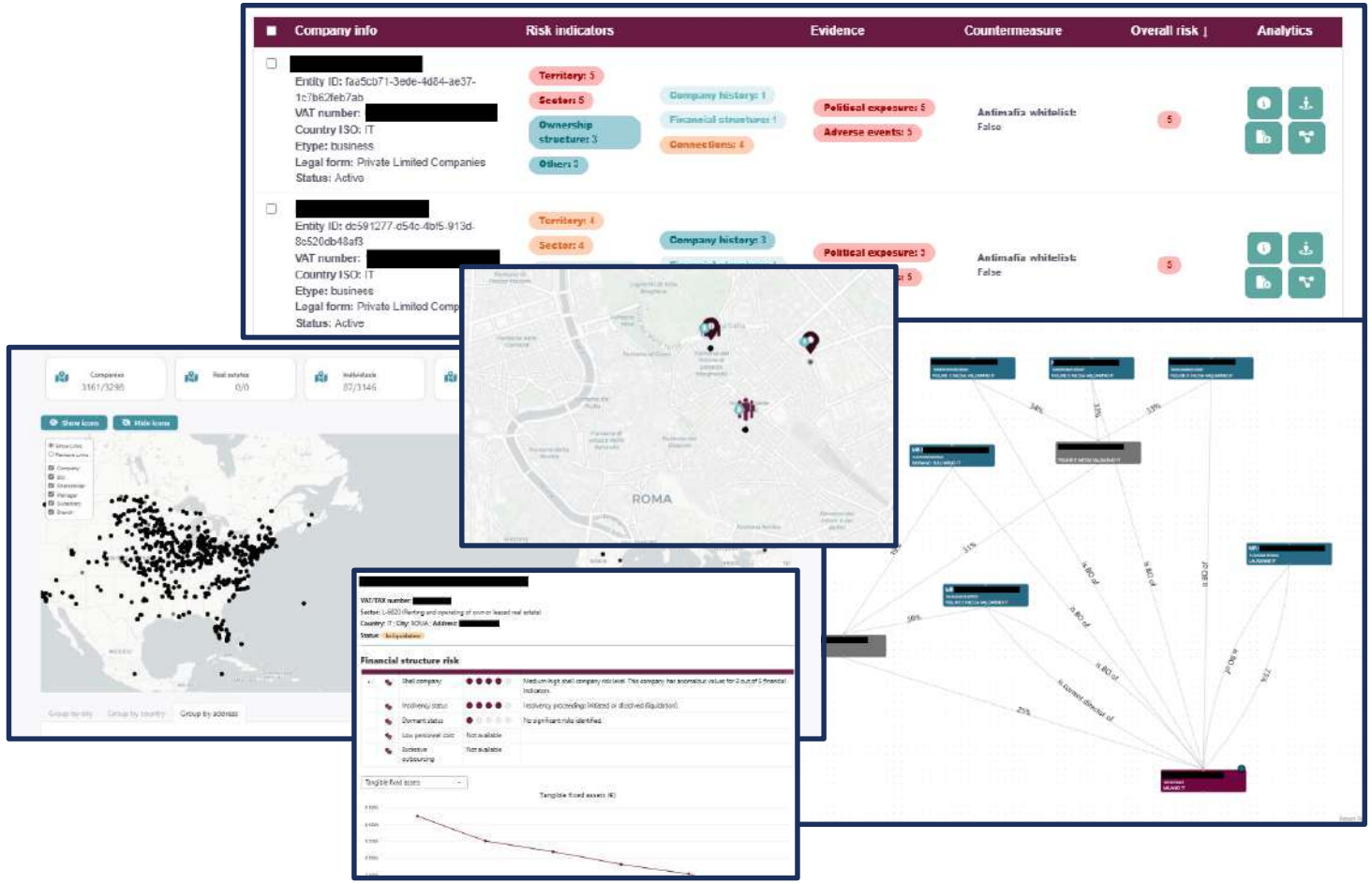
TOOL-BOX & PLATFORM

	DATACROS III
Paradigm of search	**Universal**
Type of asset	Companies, **Real Estate, Other assets**
Geographic coverage	200+ countries, 500+ mln firms
Ownership coverage	Upstream & downstream, no thresholds
Temporal coverage	Real-Time and **Historical Data**
Data sources	**20+**
Innovative risk indicators	**20+**
User Interface and visualizations	**Exportable**
API interfaces	**Yes**



TOOL-BOX & PLATFORM

- Reconstruction of **complex ownership and control networks** (including transnational chains).
- Real-time enrichment with **global coverage data**
- **Automated calculation of risk indicators**
- Identification **of high-risk addresses** and territorial clusters.
- **Visual analytics dashboards for investigations**, due diligence, and asset tracing.
- Support for case-based workflows and export/share capabilities.



USE-CASE & DEMO

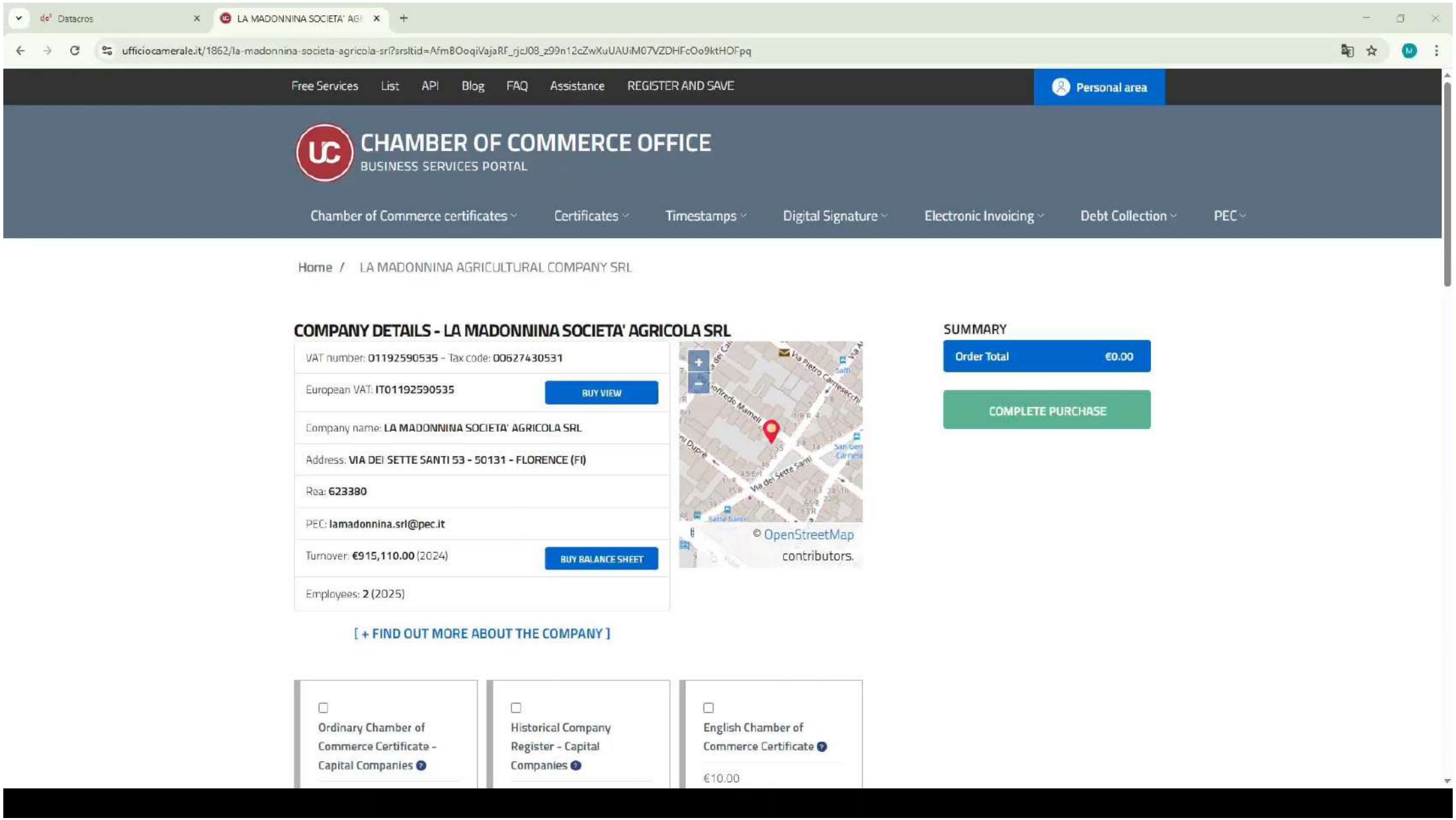
USE-CASE & DEMO

- Real investigation conducted with DATACROS III
- Control of wineries receiving RRF funds
  - Sanctioned **Russian oligarchs** are revealed **as beneficial owners**

data | cros^3

www.datacros3.com

USE-CASE & DEMO



THANK YOU

Feel free to contact us at:

MICHAELVICTOR.LOGIUDICE@UNICATT.IT
TRANSCRIME@UNICATT.IT