COMBATING FRAUD WITHIN EU COHESION POLICY WITH EMERGING TECHNOLOGIES

Webinar, 27.6.2024

Nena Dokuzov, Ministry od the Economy, Tourism and Sport, Slovenia

FACTS

1) Cohesion Policy is the EU's largest investment policy aimed at reducing economic, social and territorial disparities across Member States and regions. The financial resources allocated to Cohesion Policy amount to above one third of the EU's seven-year budget. However, due to constituting such a substantive area of the EU's budgetary expenditure, Cohesion Policy is exposed to compliance problems, as evidenced by errors (incorrect calculation or non-compliance with legal and/or contractual obligations applicable to EU's budget) and irregularities (infringements of the rules applicable to EU's budget). Particularly, fraudulent irregularities may imply serious infringements putting the credibility of the EU's Funds spending in question.

2) "Zero tolerance policy" applies to fraud affecting the EU's financial interests (i.e. EU's budgetary resources). This stands for taking necessary measures by both the European Commission and Member States aimed at protecting the EU's financial interests, including the European Structural and Investment (ESI) Funds, from fraud. Notably, prevention constitutes the first, fundamental step to mitigate the risk of fraud occurrence together with its damages to the EU's budget.

3) 'No-one-size-fits-all'

Domestic system of Cohesion Policy differs across Member States, which is determined by numerous factors, for instance the number of regions, type of governance (centralization vs decentralization), national legislative framework, division of powers between relevant national authorities. These differences reflect on various impediments to fraud prevention domestically, encompassing weak administrative capacity of a Member State's authorities, insufficient involvement of local authorities in the implementation of anti-fraud measures, complexity of national rules applicable to the ESI Funds, inefficient management and control systems. Therefore, anti-fraud measures should be adjusted to specific needs 'on the ground'.

OLAF

OLAF is part of the European Commission, but has operational independence. It receives information about possible fraud and irregularities affecting the EU financial interests from a wide range of sources, and can investigate matters relating to fraud, corruption and other offences concerning:

- all EU expenditure: the main spending categories are Structural Funds, agricultural policy and rural development funds, direct expenditure and external aid;

- some areas of EU revenue, mainly customs duties;

- suspicions of serious misconduct by EU staff and members of the EU institutions.

EDES: The Early Detection and Exclusion System is the system established by the Commission in 2016 to reinforce the protection of the Union's financial interests and to ensure sound financial management.

The EDES rules are applicable to all contracts, grants, agreements, prizes, financial instruments and remunerated experts, as well as to the implementation of the budget under indirect management.

Its purpose is to protect the Union's financial interests against unreliable economic operators by detecting and excluding them from receiving funds, and by imposing financial penalties on them. The grounds for exclusion concern: bankruptcy and insolvency situations, non-payment of taxes or social security contributions, grave professional misconduct, fraud, corruption, participation in a criminal organisation etc., serious breach of contract, irregularity, entities created with the intent to circumvent fiscal, social or other legal obligations (creation of shell

ECA Report

Tackling Fraud in EU Cohesion spending: managing authorities need to strengthen detection, response and coordination

Main findings:

- Managing authorities generally have no specific anti-fraud policy

- Managing authorities systematically assess fraud risks, but this process could be further improved

Example: Stock taking study on preventing fraud and corruption in the ESIFs

The study was based on a sample of 50 2014-2020 OPs (41 of which related to Cohesion, excluding ETC) selected by the Commission on a judgemental basis to cover all Member States and a range of sectors and funds. The study team reviewed information from Member States (in particular the outcome of their fraud risk assessments) and conducted interviews with programme authorities and AFCOSs.

Positive remarks	Areas for improvement	Potential Digitech contribution
Anti-fraud and anti-corruption efforts are more formalised and systematic in the 2014-2020 programming period.	Proportionateness of mitigating measures is lowest for the risks of collusive bidding and double funding.	Data definition: (i) identification of data sources, (ii) examination of data sources, (iii) encryption of the data, (iv) transmission of the data, (v) use of the data
Mitigating measures are generally proportionate to the self-assessed risks.	Some authorities may underestimate their self-assessed levels of fraud risk.	Upon the data recognition: (i) identification of the potential risks, ii) creating measures for risk mitigation
Most authorities are using the Commission`s fraud risk assessment template.	Not all managing authorities conduct a fraud risk assessment at OP level.	Generative data solutions for national data basis versus predictive data solutions based on common EU tool
A more inclusive fraud risk assessment process is better suited to reducing fraud risks.	There is a need for more communication to Member State authorities on anti-fraud activities. In its current form, the managing authorities in the sample perceive Arachne as not entirely meeting their needs.	Decentralized interoperable communication platforms operating on federated distributed manner for facilitation of the risk mitigation and anti-fraud measures implementation.

ECA Report

Tackling Fraud in EU Cohesion spending: managing authorities need to strengthen detection, response and coordination

Main findings:

- Managing authorities have improved their fraud prevention measures but made no significant progress towards proactive fraud detection

- Managing authorities systematically assess fraud risks, but this process could be further improved

Example: Innovative fraud prevention measures: Integrity pacts

In 2015 the European Commission and Transparency International, a global nongovernmental organisation actively fighting corruption and particularly known for its publication of the Corruption Perception Index (CPI), launched a pilot project on 'integrity pacts' as an innovative way of preventing fraud in EU cohesion policy projects. An integrity pact is an **agreement in which the authority responsible for awarding a public contract and the economic operators bidding for the contract undertake to abstain from corrupt practices and ensure transparency** in the procurement process. Pacts also include a separate agreement engaging a civil society organisation (such as an NGO, a foundation or a local community-based organisation) to monitor all parties' compliance with their commitments. The purpose of integrity pacts is to **increase transparency, accountability and good governance** in public contracting, enhance trust in public authorities and promote cost efficiency and savings through better procurement.

Key point: how to integrate advanced digital technologies into the fraud detection processes with regard to data analytics?

Emerging technologies respond to anti-fraud actions

Tackling Fraud in EU Cohesion spending: managing authorities need to strengthen detection, response and coordination

Strengthening detection:

Authentication process: Creation of data labels for digital objects, proving product authenticity and destination. Enrich existing digital twin information in a technology neutral approach (e.g. Digital Product Passport). A new channel for consumer engagement.

Relevant technologies?

Response

Links the physical serialisation to the digital twin of the product. Enables a dynamic check of a brand's digital identity and product information. Built to easily integrate additional authentication and anti-tampering services.

Relevant technologies?

Coordination

Create a network with the different parties in the supply chain to onboarding of the costs.

Facilitate and expedite data onboarding processes.

Share trusted information to strengthen the risk analysis systems

Relevant technologies?

Emerging technologies respond to anti-fraud actions

Examples:

AI-driven fraud prevention:
Dynamically detect and stop fraudulent payments by scanning against a wealth of past data. PaymentGuard uses machine learning to reference a historical database of customer data – including transactions, device information, and geolocations – to intelligently model existing and emerging patterns. These patterns predict trends as they occur, and generate instant alerts that can be processed using a sophisticated-yet-simple case manager.

Machine Learning for Forensic Accounting and Financial Investigations
Use of leading cloud-based technology to automate the extract, transform, and load (ETL) processes of investigations from structured or unstructured data sources and investigative algorithms. Prior to these recent technology advancements, the ETL portion of engagements took a substantial amount of budget—sometimes even as high as 50%. Although the result of the ETL processes typically took on a form consistent across engagements, the ingestion portion of the ETL processes would have to be custom scripted for each engagement. Utilizing machine learning and artificial intelligence, today's tools provide full automation of the ETL processes as well as various analytics and behavior algorithms that allow for customized testing and flexible reporting

Emerging technologies respond to anti-fraud actions

Examples:

Benefits of Blockchain in Fraud Detection and Prevention:

While the uses of blockchain are often associated with supporting blockchain transactions, the powerful role of blockchain in the business world extends far beyond cryptocurrencies. One of the areas where blockchain technology can have a significant impact is fraud detection and prevention.

- **Immutable ledger:** Immutability is one of the most significant use cases of blockchain, making it a revolutionary technology for fraud detection and prevention. Once data or transaction is stored in the block, they can't be modified, altered, or removed. It means any suspicious attempt to tamper with the transaction will be detected and prevented in real time, making it intimidating for fraudsters to exploit the vulnerabilities.
- **Transparency:** Transparency is another remarkable feature of blockchain, making it an effective technology in fraud detection and prevention. Since all the transactions in the blockchain are visible to every member with permission, any changes to the ledger are recorded in real-time and visible to everyone. So, if anyone tries to tamper with the data, their attempt will be detected immediately, and they can't carry out their fraudulent activities.
- **Decentralized Nature:** Blockchain is a decentralized, distributed digital ledger that records data and makes it visible to all authorized members. In the decentralized network, only authorized persons from different departments can access, share and control current and previous data. It enables all authorized members to detect faulty transactions without needing a central authority, preventing possible human errors, frauds, and waste of time.
- **Smart Contracts**: Blockchain facilitates smart contracts, which are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. The smart contract triggers an