



Preventing financial crime

– how to increase the effectiveness of the regulatory system?

Natalia, Competency Center Director
Ewa, Offering Lead



Table of contents

Introduction	3
Estimated size of the underground economy in Poland	3
Actions taken by supervisory bodies	5
On the effectiveness of the system for counteracting financial crime	6
How does the current system work?	7
Is a compliance-based approach enough?	8
Conclusion	10
Benefits from the cooperation with Sii in the area of KYC/AML/CFT	11

“Insanity is doing the same thing over and over and expecting different results.”

Albert Einstein

Introduction

When operating under the same scheme over and over again, can we expect varying results?

The regulator introduces regulations and supervises their implementation. The obliged institutions implement regulations and take actions aimed at avoiding penalties imposed on them by the regulator. Criminals operate freely, adapting their M.O. in an agile manner to the changing regulatory reality.

How do we step outside the bounds of the current system?

My suggestion: let's change our professional mindset.

Joanna Kwaśniewicz

KYC/AML/CFT Expert at Sii Polska

[Check Sii's KYC/AML/CFT offer](#)



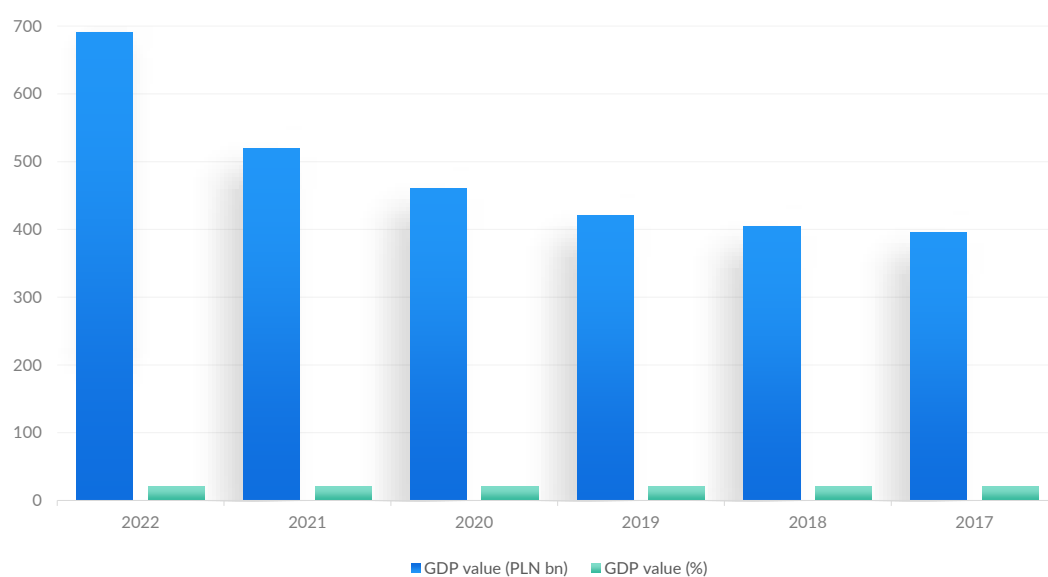
Joanna, KYC/AML/CFT Expert

Estimated size of the underground economy in Poland

According to estimates, the underground economy, also known as the shadow or black economy, in Poland will grow to PLN 590 billion in 2022. It is worth noting that its size has remained at 18% of

GDP for many years, but in terms of value, it has been steadily growing (from PLN 397 billion in 2017 to the indicated estimate of PLN 590 billion for 2022).

Size of the underground economy in Poland (2017-2022)

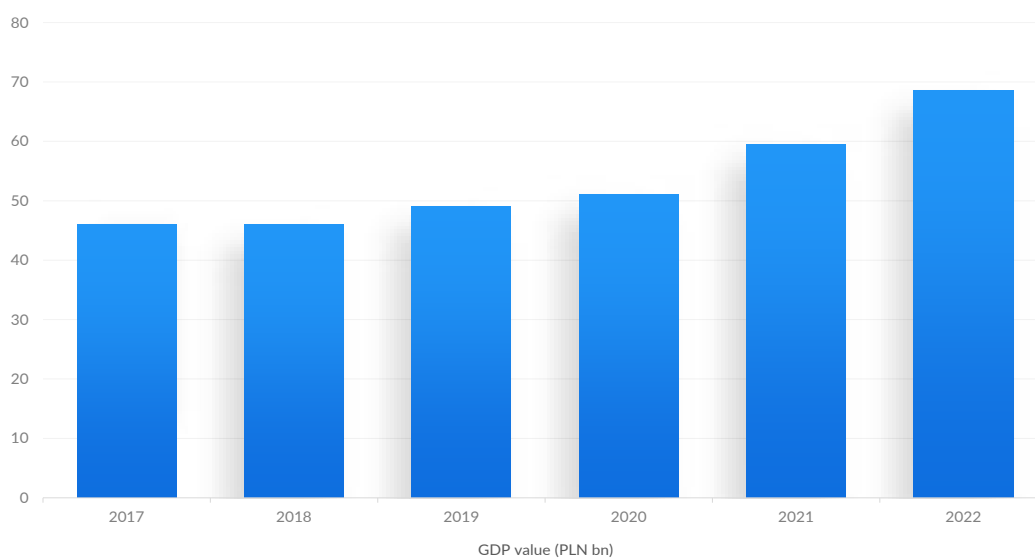


(Data source: Arkadiusz Matusiak, Wolf Theiss, P. Daszkowski Ltd.)

Financial crime within the underground economy related to the broader KYC/AML area is respectively (as estimated in 2017, as a percentage of the amounts indicated above):

- money laundering - 4.5%,
- extortion - 3.5%,
- corruption - 3.5%.

Estimated size of the underground economy in Poland (2017-2022)
(areas: money laundering, extortion, corruption)



(Data source: Arkadiusz Matusiak, Wolf Theiss, P. Daszkowski Ltd.)

Actions taken by supervisory bodies

According to the data issued by the General Inspector of Financial Information (GIFI) for 2021:



The number of descriptive notifications from the obliged institutions is 3574 (3852 including other sources).



The total amount of suspected criminal assets amounted to approximately PLN 8.5 billion.



The obliged institutions reported more than 36.7 million over-threshold transactions.



The GIFI has blocked 1426 accounts with funds of a total value of about PLN 172 million and suspended 50 transactions with a total value of PLN 7.1 million.



In 2021, the GIFI initiated 2442 analytical proceedings based on the submitted information.



In 2021, the GIFI carried out 9 inspections based on the AML Act.



As a result, the GIFI submitted 519 notifications on suspicion of a crime.

By the provisions of the AML Act, authorized supervisory bodies also conducted audits within the scope of their competence:



The National Bank of Poland conducted 556 inspections of exchange offices.



Ministers, voivodes, and heads of districts have carried out 24 inspections in foundations and associations.



The Financial Supervision Commission conducted 12 inspections.



Customs and Tax Offices have carried out 27 inspections.



The National Cooperative Savings and Credit Union carried out 8 inspections in the liable Cooperative Savings and Credit Unions.



Presidents of Courts of Appeal conducted 62 inspections of notary offices.

This means that a total of 689 inspections were conducted. Taking into account the size of the underground economy in 2021, i.e. PLN 511 billion, and assuming that the three types of financial crime mentioned above account for 11.5% of this amount (i.e. PLN 58.8 billion) – can we consider the actions

of the system (blocking of accounts to the amount of PLN 180 million and notices of suspicion of crime with a financial value of PLN 8.5 billion) to be effective? Do they actually counteract financial crime and meet the objectives of the regulations?



BPO Team

On the effectiveness of the system for counteracting financial crime

Perhaps we should risk a conclusion that financial crime still pays off because the actions of the system are not adequate (in terms of quantity and, above all, value), offensive, and do not truly counteract the negative phenomena?

Counteracting financial crime (fraud, money laundering, corruption) from the perspective of an obliged institution equals new regulations and new obligations. Implementing regulations requires knowledge, competencies, and resources.

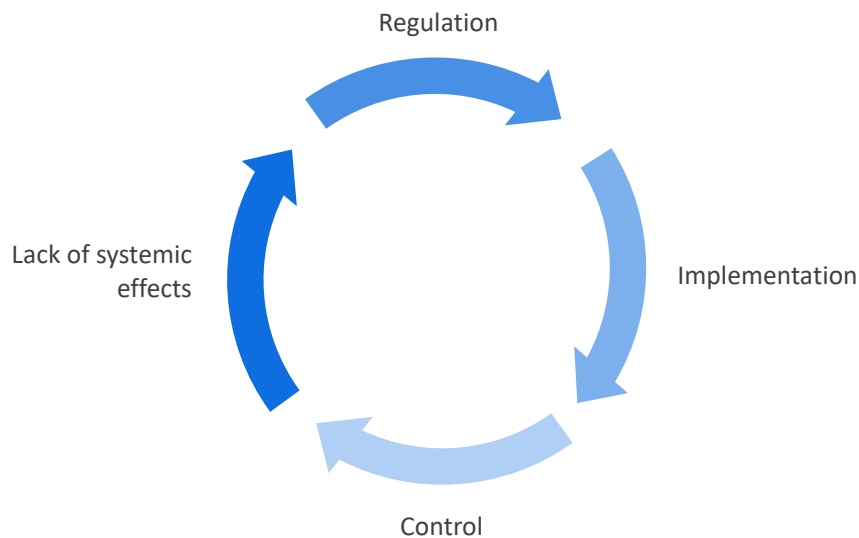
What does it mean for the obliged institution? First of all, time for implementation and costs, costs, costs. Taking the above into account, I would like to pose a seemingly anarchist question –

is the system effective?

As professionals, we increasingly get the impression (although we prefer not to admit it out loud) that the area is over-regulated. New regulations are appearing more and more frequently, and shortly, the establishment of the European Anti-Money Laundering Authority (AMLA), will probably result in clarifying the current regulations and interpretations and implementing new ones.

However, despite the more and more detailed regulations, which impose new obligations and cover a wider range of activities of the obliged institutions, counteracting the negative phenomena does not bring the expected results.

How does the current system work?



Financial crime prevention system operations scheme

The regulator implements the regulation and controls that it is implemented correctly. Then, the obliged institution implements the regulation and takes action to avoid a possible penalty for non-compliance

with the regulation. Thus, it is clear that the system focuses only on the regulation, its implementation, and controlling compliance. In short, **the system is focused on itself.**



Who then prevents financial crime (money laundering, terrorist financing, fraud, and corruption)? It seems that nobody does:

- Regulator focuses its activities on the mandatory institutions.
- Obligated institutions focus their activities solely on compliance with the guidelines of the regulator.
- Regulation proves ineffective, so the regulator makes it more specific.

In other words, the regulator takes another ineffective action. The obliged institutions implement them. All participants in the system are so focused

on regulations that no one is actually concerned with preventing financial crime, to which the entire system is supposedly dedicated.

Is a compliance-based approach enough?

So is the compatibility criterion sufficient on its own? I would argue that it is not. Can we do something about it? In my opinion - yes. First of all, it is necessary to go beyond the regulatory minimum.

It is an open catalog, which does not close the possibility of action, as long as these actions remain within the limits of the law.



Start thinking like criminals.

1. Think outside the box.
2. Think boldly.
3. Look holistically.
4. Pay attention to details.
5. Recognize the non-obvious.
6. Create scenarios.
7. Validate scenarios.
8. Explore new scenarios.
9. Use imagination.



Engage people. Enable them to step outside the box.

Do not confine them to strict regulations and „from-to“ manuals. An informed and educated employee is the greatest value in an organization.

An employee who is:

1. Competent
2. Meticulous
3. Independent
4. Courageous
5. Open-minded

will be like a **poacher** - will go hunting, set snares, act proactively, offensively, and unconventionally (under and within the law). They will identify every new scenario. They will not allow risks to materialize. They will be where the criminal does not expect them to be.

An employee who is:

1. Competent
2. Meticulous
3. Dependent
4. Intimidated/scared
5. Bureaucratic

will be like a **gamekeeper** who knows the regulations and moves only within them. They will keep an eye on the forest, but while working only with the patterns they know, they will not see new threats. And criminals, who are equally familiar with regulations and guidelines and, additionally, are agile in adapting to legislative reality, will appear in the least expected time and place. The risk will materialize. And what is worse, it may go unnoticed, which will weigh on the effectiveness of the entire system.

(Poacher vs. gamekeeper – based on Lee Byrne FLPI, CITF, AdvCertVC, Great Chatwell Academy of Learning)



Make sure that we have the support of:

- IT systems, i.e.:
 - a) Custom rules
 - b) Dedicated solutions
 - c) Out-of-the-box solutions
- Internal lists
- Industry lists
- Commercial lists
- Media information (primarily from online sources)
- Open-source intelligence
- Open-source intelligence
- Linked databases
- Business intelligence

And if there is an additional need, also use:

- Investigation services
- Field inspections helping to assess: human resources, premises, equipment, and machinery park of the contracting party



Use the experience of others, learn from (their) mistakes and take advantage of the knowledge and expertise of third-party professionals.

Conclusion

It seems that going beyond the regulatory minimum and the compliance criterion are additional activities, generating excessive costs. However, we should consider not only compliance with regulations but also the effectiveness of the system.

The quote at the beginning of the article is not accidental, because, in the absence of effectiveness, further regulations, interpretations, and further specifications (entailing additional costs for the obliged institutions) appear more than likely.

Therefore, would not something that seems to be an idealistic approach today – bold actions taken by the obliged institutions, going beyond the regulatory minimum (but remaining in compliance with the law) that eliminate or significantly reduce financial crime be ultimately more effective, and thus cheaper?

The system would have a chance to work.



Damian, Analyst

Benefits from the cooperation with Sii in the area of KYC/AML/CFT

We offer professional support for your company within the field of ensuring compliance with regulations and simultaneous cost optimization. The scope of Sii's services within the field of Know Your Customer (KYC), counteracting money laundering (AML), and financing terrorism (CFT) includes:

- **250+ experts** – the support of consultants, analysts, data quality specialists, and dedicated teams of specialists.
- **Process and cost optimization** through a combination of business know-how and technology
- **Gaining control and transparency in KYC/AML processes.**
- **Strong experience** in the banking and insurance sectors.
- **Multiple cooperation models** – experts outsourcing, management of compliance and customer verification processes, process audits.
- **Compliance with the highest security standards** confirmed by ISO 27001 and ISO 9001 certificates.
- **Flexibility and fast time-to-market** – starting the project even within 3 weeks
- **Automation of processes and adjusting them to regulations** required by national and European institutions.
- **Outsourcing in an onshore or offshore model** based on pre-defined KPIs and agreed SLAs.
- **Complementary services and tools** – back office support, class-A offices, IT tools, and Service Desk.

Are you looking for support? Contact Sii!

Get expert support in the field of compliance and reduce operational costs. Discover the full scope of Sii's KYC/AML/CFT services or contact us.

Get to know our offer

With 7 000+ specialists, Sii is the largest technology consulting, digital transformation, BPO and engineering services vendor in Poland. Sii experts carry out projects for leading companies operating in the automotive, banking and financial, hi-tech, healthcare, retail, logistics and utilities sectors. Sii Poland has 15 offices in Warsaw, Gdansk, Wroclaw, Poznan, Cracow, Lodz, Lublin, Katowice, Rzeszow, Bydgoszcz, Czestochowa, Pila, Bialystok, Gliwice and Szczecin.