



Deloitte Forensic in Ukraine and the CIS
Business Intelligence
Services Capability
Statement

Introduction	03
Deloitte Forensic in Ukraine and the CIS	04
Integrity due diligence	05
Review methodology	06
Compliance screenings	07
Lifestyle review	08
Forensic Revolver	09
Analytical procedures	10
Whistleblower hotline	11
Compliance trainings	12
Our experience	13
Our team	14

Introduction

We are the leading Forensic practice in Ukraine and the CIS. We offer the full range of Forensic & Dispute services, enabling our clients to adjust to a myriad of day-to-day changes and unforeseen circumstances.

With over 85 full-time professionals across the region dedicated to Forensic work, we lead our competitors in both scale and focus.

Deloitte Forensic in Ukraine and the CIS



Business Intelligence: defense of your business

Our business analysts team has a wide experience in obtaining and analyzing of information. Our analysts use advanced methods for conducting research to identify risks of unreliability.

- We perform **integrity due diligence** one-time as well as on regular basis within complex compliance programs.
- We use **analytical software** for review of big data and identifying potential fraud and reputational risks.
- We launch **independent hot lines** and conduct **trainings for compliance specialists**.

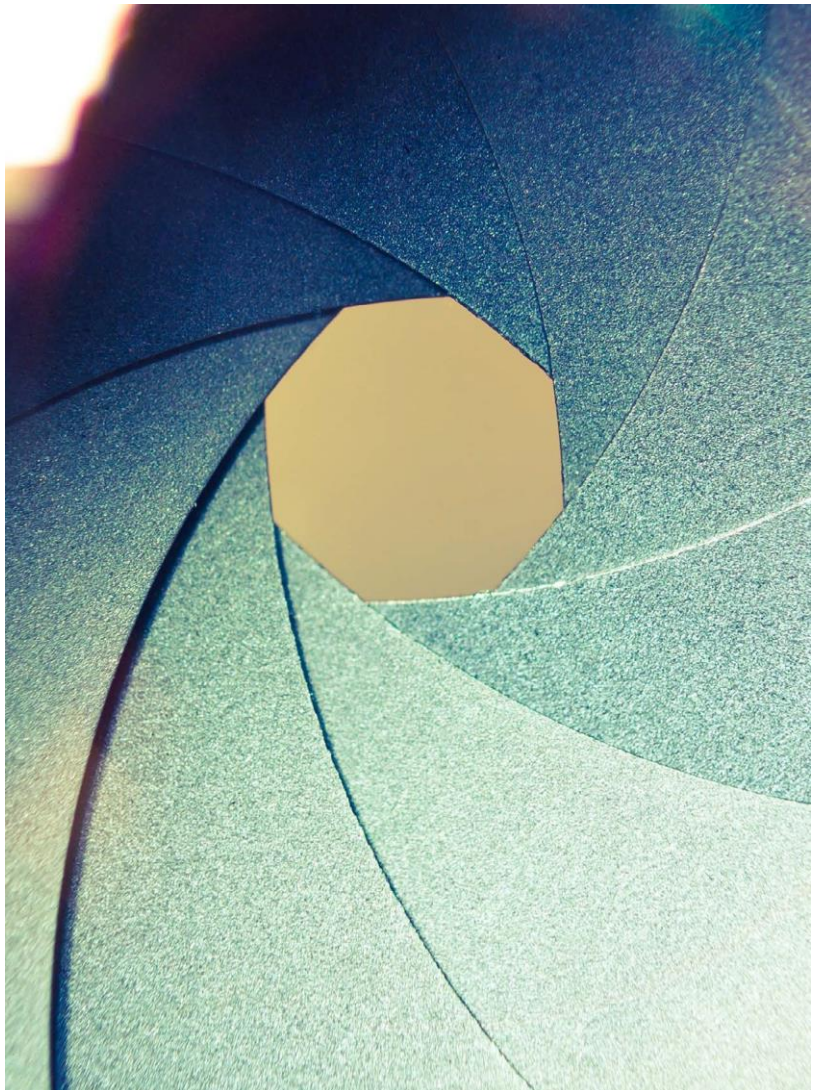
Integrity due diligence

“Although most managers are aware of the inherent risks associated with using vendor products and services, many do not have the necessary processes or controls in place to address such risks. But in today’s increasingly globalized world, such preventive measures matter more than ever.” - ACFE

Doing business in Ukraine carries specific risks arising from the general lack of transparency and pervasive perceptions of corruption. If these risks are not mitigated before a relationship is formed, an organization may face a financial loss, reputational damage and/or civil and criminal liability, including regulatory sanctions.

Integrity due diligence (IDD) is an in-depth study of a target’s reputation, business activities, ties and connections, aimed at establishing that there are no hidden reputational risks associated with the target.

Conducted with respect to clients’ agents, their business partners or their acquisition or investment targets, and tailored to meet our clients’ specific requirements, our work is performed using a proven methodology under the strictest confidentiality and in compliance with the boundaries of the applicable Ukrainian law.



Review methodology

We have a wealth of experience with performing in-depth background research in Ukraine and the CIS. We understand the business environment in the region and are skilled in locating relevant, difficult-to-find information.

Our expertise

- Our team has extensive experience not only in selecting and using reliable sources of information, but also in putting into the proper context any controversial information found in questionable open sources.
- We have access to public public and subscription-based databases, such as corporate registries, press and court archives, and international compliance databases.
- Our expertise enables us to determine the quality and timeliness of information, and to cross-check it against different independent sources.

Our network

- We only use trusted sources that have been carefully selected and vetted.
- All our sources are required to operate in accordance with Deloitte's standards of confidentiality and ethical behavior.



Business activity, corporate structure, principals and shareholders



Potential red flags: evidence of corruption and other fraudulent activities



Former customers and projects, experience and track record



Connections with state-controlled companies, the Government and/or politically exposed persons (PEPs)



Hidden influence – potential beneficiaries and related parties



Evidence of aggressive tax optimization, financial stability



Compliance screenings

Many of our clients have obligations under international Anti-Bribery and Corruption legislation to conduct due diligence into their counterparties. We can help them to assess risks posed by specific counterparties, using a tiered approach designed to deploy resources in proportion to the integrity risk posed by each counterparty.

Level 1

Targeted searches of adverse public domain information pertaining to the counterparty in order to identify any “red flags”:

- Verification of any information provided by the counterparty to the client
- Identification of any controversies or allegations of impropriety involving the counterparty or its principals
- Identification of any significant litigation proceedings
- Determination of whether the counterparty is included in any international sanctions lists
- Determination of whether any key principals are listed as PEPs

Level 2

Comprehensive review of public domain information (positive, negative or neutral):

- Review of the company’s formation and history
- Brief profiles of key principals, describing their corporate affiliations and professional reputation
- Assessment of the media profile and commercial reputation of the counterparty, especially with regards to its business practices and relationships with partners
- Identification of key business partners (customers and suppliers)
- Contextual analysis of any “red flags” identified in the course of research
- Overview of the counterparty’s litigation record, with a focus on any significant cases that might pose a reputational or commercial risk to the counterparty
- Review of sanctions and PEP list checks

Level 3

In-depth review using both public domain and private sources of information, covering the scope of Level 2, supplemented by enquiries among confidential sources. These enquiries will seek to:

- Determination of whether there are any “red flags” relating to the company not found in the public domain
- Clarification of any issues of concern found in the public domain
- Determination of whether there are any allegations of impropriety not in the public domain
- Filling in of any gaps in the public record pertaining to the counterparty, such as any periods of inactivity
- Site visits in cases where there are indications that the company may not be a genuine commercial entity

Lifestyle review


Based on our experience, one of the most telling indicators of fraud is a discrepancy between an employee's income and his expenses. Lifestyle review reveals such discrepancies through targeted searches focused on:

Lavish spending

We review social networks, media databases and other public domain sources for any examples of extensive spending and luxurious lifestyle of the Target and his/her family members.

Ukrainian assets

We compile a list of the assets identified in the course of public domain review and identify their potential value through official disclosures and online sources.



Lifestyle review seeks to locate the Target's property and assets, including the assets that may be held by his/her relatives on his/her behalf.

Foreign assets

Further, we identify jurisdictions frequented by the Target and search available local public records for businesses, property or registered family members.

Source enquiries

In many cases, a review is supplemented with enquiries among trusted local sources. We take all precautions in order not to let a Target know about an ongoing investigation.

Forensic Revolver

Forensic Revolver is an express diagnostic tool used to identify potential conflicts of interest and business risks associated with the Client's counterparties. Forensic Revolver uses sophisticated data mining tools developed by Deloitte specialists.

Our approach

Revolver involves the data mining of a combination of the following:

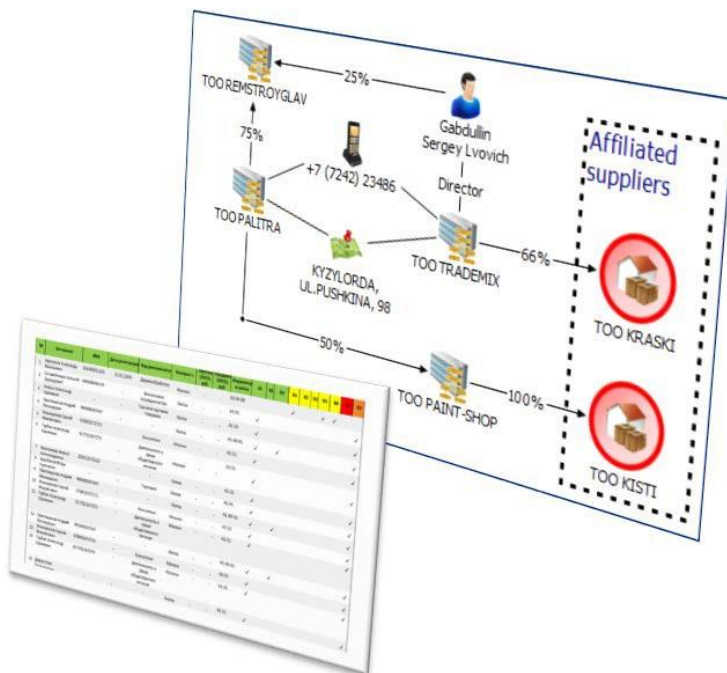
- A limited amount of counterparty data (name, tax identification number, turnover with counterparty and date of first transaction);
- Employee details (surname, name, patronymic and start date);
- Publicly available corporate information, which we obtain electronically.

Our expertise

Our specialists use different public sources of corporate information in Ukraine and other CIS countries on a daily basis; thus they know the specifics of available data.

Based on our experience with corporate investigations, we have worked out a unique risk matrix to identify paper companies and companies potentially involved in fraud schemes.

Revolver uses specialized IT technologies initially developed for law enforcement authorities. We base our IT tools on such technologies, but have configured and adapted them to corporate investigations.



Analytical procedures

Using data provided by the Client, we will collect all necessary information from relevant public sources in electronic form and conduct automated tests with specialized IT tools. We will provide a report in English or Ukrainian setting out the results of our tests. The report will identify risks and gaps, and will contain our recommendations for the Client going forward. We will include tables and visual charts detailing our findings.

Information collection

- We collect information on the Client's counterparties from web-based sources
- Collating open-source data and information from the Client's EPR systems, we create a standalone database to run tests.

Data-driven tests

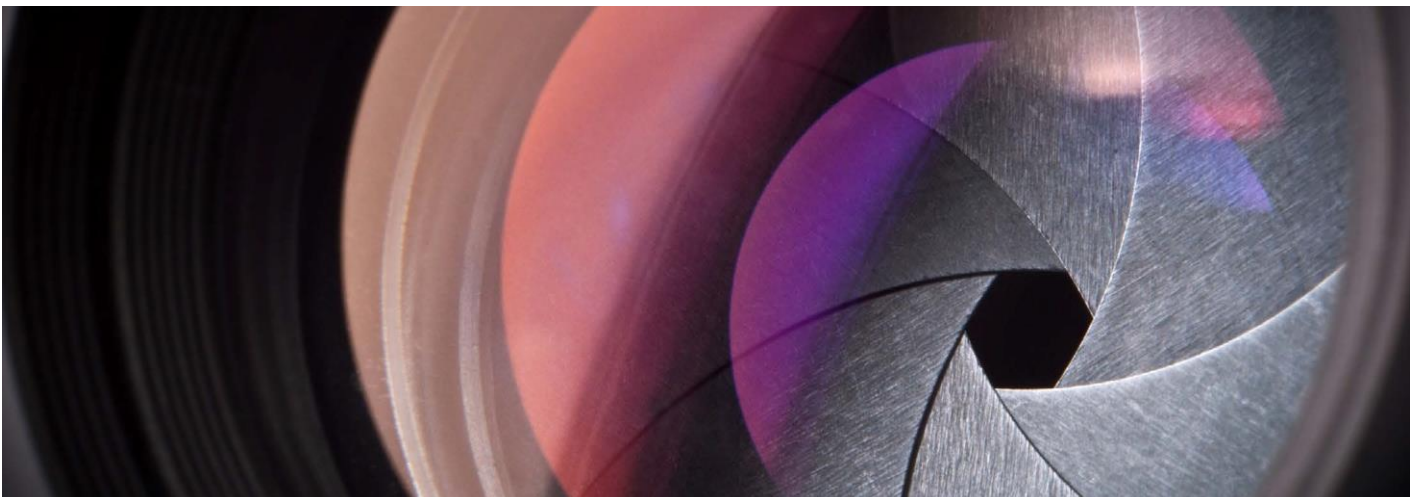
- Using sophisticated technology developed by our professionals, we test the data against a number of risk indicators.
- Risk indicators are tailored to meet the needs of every project.

Risk assessment

- Compiling the results of data-driven tests, we calculate counterparty risk scores and assign them to particular risk groups based on the evaluation.
- We supplement the automated test with visual link analysis to identify potential networks of interconnected counterparties.

Results and deliverables

- Our deliverable is a written report with key findings and recommendations, supplemented by visual representation of our findings.
- The report is supplemented with spreadsheets containing complete risk profiles of all the counterparties analyzed, which can serve as a valuable resource for security and compliance specialists.



Whistleblower hotline

What forms can it take?

- An email account set-up as a tool for an organization's employees and other stakeholders to report their concerns regarding potential misconduct at the workplace
- Website which registers incoming messages (similar to <http://demo.deloitte-hotline.ru>)
- A dedicated phone line attended to by experienced forensic specialists during business office hours (local time); automated answering machine outside of office hours. All messages are to be recorded for quality control purposes

Who is it for?

- Employees, management and shareholders
- Vendors, customers and third parties

What is the time frame?

- Email is provided upon the contract being signed.
- If the client needs a customized website (with the client logo, etc.) the time frame can increase by 1–2 weeks.

What is the result?

- A detailed report after each incident reported via the email or phone hotline with a description of reported circumstances
- A quarterly report providing statistics and key details of reported incidents

Having a whistleblower hotline that is easily accessible and trusted by employees and other stakeholders is critical to an organization's overall compliance program and bottom line.

Deloitte's whistleblower hotline service provides a safe and secure means of reporting concerns of potential misconduct, while providing the organization's management with timely reports of such incidents and a comprehensive summary at the end each quarter.

Compliance trainings

We provide IDD training programs for compliance employees tailored to the needs of specific business areas. All our instructors are active practitioners with an abundance of hands-on knowledge, who provide real-world examples throughout these seminars. Our training programs cover the following areas:

Research methodology

- Strategic intelligence and cognitive bias
- Assessing source reliability
- Cross-checking between sources
- Effective search tools
- Working with social networks

Forensic technology tools

- Data mining
- Visual link analysis
- Software for analyzing corporate information
- Preserving electronic evidence

Public domain sources

- Ukrainian and international corporate databases
- Official disclosures, state tender records
- CIS litigation records: availability, search options
- International compliance databases
- Media subscription databases

Our experience

Controversial business partner

We were engaged by a Japanese multinational corporation to investigate concerns regarding alleged political exposure of a local oil-and-gas group as well as its relations with a controversial businessman. Our investigation revealed that the group was distancing itself from the non-transparent local market and, as a result, was less exposed to business risks. Though we did not identify any explicit instances of political support rendered to the group by its alleged political advocates, we detected indications of potential abuse by the Target of its relationships with state-owned oil companies to gain unfair advantage.

Offshore network

As part of an audit, a Hong Kong-based fish processing conglomerate surveyed its suppliers and CIS fishing industry operations. The client wanted to review the transparency of purchases from its local partners.

Based on data from corporate and judicial registers, we identified a number of affiliated legal entities in CIS and offshore zones that could have been used for generating illegal profits. Media sources mentioned that the business partners were accused of breaching antimonopoly legislation.

Cross-jurisdictional mass counterparty screening

At the request of a global telecom company, we reviewed over 3,000 its business partners and 6,000 employees in three jurisdictions: Kazakhstan, Ukraine and Kyrgyzstan. Our analysis helped identify potential conflicts of interests between the Client's employees and business partners, including cross-jurisdictional links. We also assessed the counterparties for potential fraud risk. For this purpose, our team worked together with the client to develop customized risk criteria ("red flags").

Real estate lease price overstatement

Major retail chain requested that Deloitte conduct automated analysis to reveal potential relationships between property lessors that could have resulted in overstatement of lease rates. The client provided us with a list of leased properties and their lessors, as well as contact details of the lessors and their representatives.

In result, we identified large groups of leased properties potentially controlled by related parties (the largest group consisted of 70 stores). Our analysis also showed that in some regions over 20% of leased stores were owned by the same owners, which might have hampered competition on the lease market.

Our team



Alexander Sokolov

Partner

Deloitte CIS

Tel: +7 (495) 787 06 00

ext. 3095

Fax: +7 (495) 787 06 01

alsokolov@deloitte.ru



Dmytro Anufriev

Partner

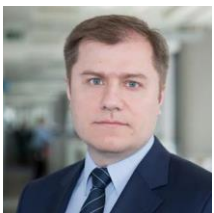
LLC "Deloitte & Touche"

Tel: +38 (044) 490 90 00

ext. 2622

Fax: +38 (044) 490 90 01

danufriev@deloitte.ua



Maxim Fedotov

Senior Manager

Deloitte CIS

Tel: +7 (495) 787 06 00

ext. 5396

Fax: +7 (495) 787 06 01

mafedotov@deloitte.ru



Viktoria Samoilenko

Manager

LLC "Deloitte & Touche"

Tel: +38 (044) 490 90 00

ext. 3668

Fax: +38 (044) 490 90 01

visamoilenko@deloitte.ua

deloitte.ua

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 244,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.