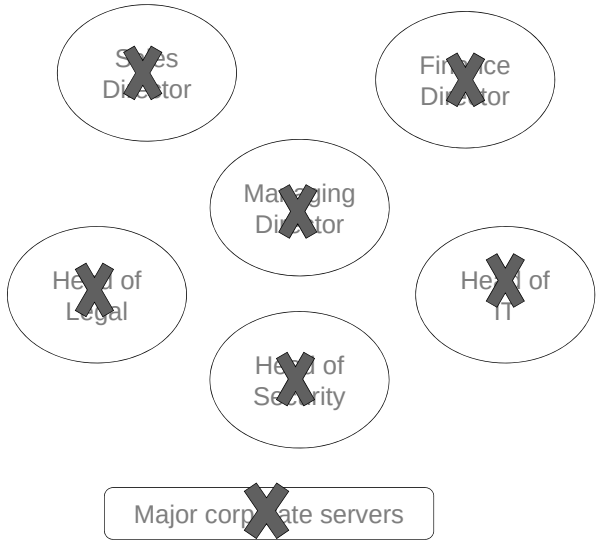
Conducting Effective Compliance Investigations in Russia & CIS

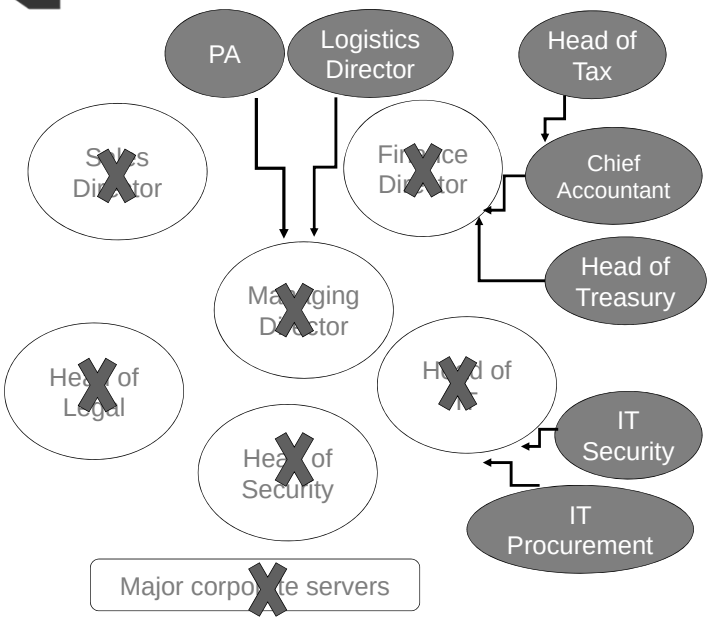


Case study 1: When all people have gone…

TOP 3 IT company in the CIS region
New shareholder decided to change the management
Then a major compliance review was announced…

Initial findings:

- Company loss of over EUR 50 mln, allegedly caused by the management;
- Wrong accounting records for the last several years;
- Lack of key management's corporate devices and mail servers;
- Lack of employees' trust and loyalty to the new management;
- No working compliance procedures in place.



Case study 1: When all people have gone…

Done:
Over 30 employees from the entourage;
Over 50 devices collected and imaged;
Over 30,000 paper documents digitized and uploaded to E-Discovery Platform;
Over 3 Tb of information analyzed and…

Results of analysis:

- Management's personal banking accounts in Switzerland and France;
- Real-estate property in EU and US;
- Acquisition of luxury goods;
- Financing of personal spending at the expense of the company;
- Assets withdrawal to third parties, including nominees;
- Evidence of intent;
- Increase of employees' trust and interest to compliance.

Compliance Investigations

CIS challenges

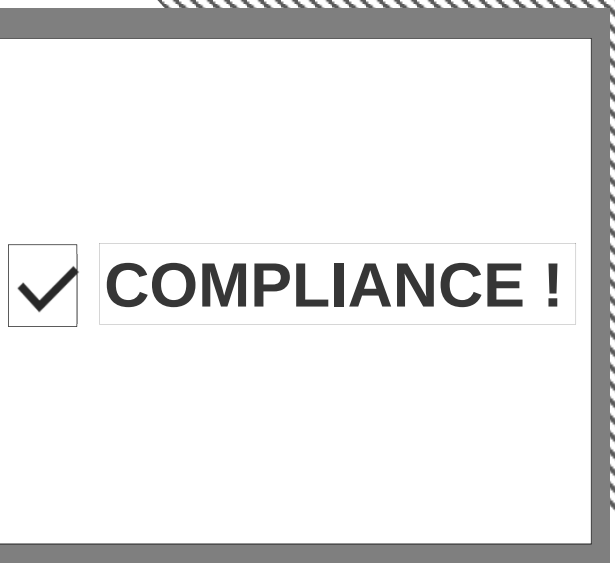
1. **Major focus on fraud matters, rather on unethical behavior or misconduct.**
2. **Lack of compliance culture / understanding among employees.**
3. **Lack of really working compliance procedures.**
4. **Whistleblowing is considered in a negative context in certain regions.**
5. **Complexity of law enforcement.**

COMPLIANCE?

Compliance Investigations

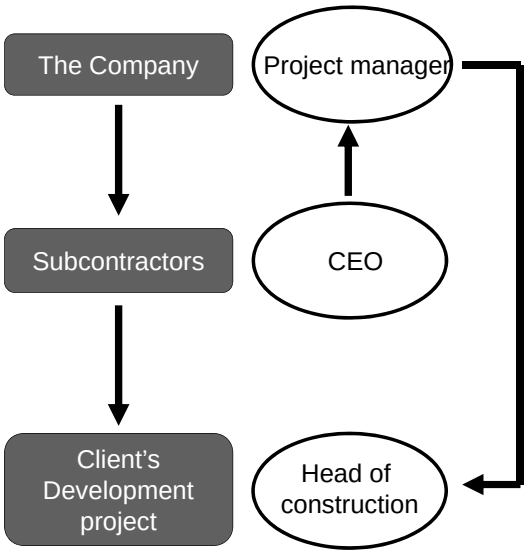
Meeting the CIS challenges

1. **Talk to the decision makers first.**
2. **Explain your purposes to employees.**
3. **In general people don't like fraud – ask for support.**
4. **Be creative. Use modern technologies.**
5. **Take actions against identified misconduct and fraud and communicate the results to employees.**
6. **Keep in mind counteractions from investigation targets.**



Major corporate corruption schemes in CIS

1. Management runs similar parallel business utilizing the company's resources and clients. The parallel business usually registered on relatives, friends or dependent people
2. Management withdraws money via contracts with affiliated or controlled entities, which are suppliers or distributors of the company.
3. Kickbacks from suppliers to decision makers and contract holders.
4. Lending money to affiliated companies on non-market terms.
5. Cashing out money via salary payments to "Dead Souls" or to non-citizen employees.
6. Selling corporate assets on undervalued prices to affiliated buyers.
7. Payments for not provided services or goods. Inflation of prices.
8. Procurement process manipulation to onboard "friendly" supplier.
9. Facilitation payments to state officials for obtaining approvals, permissions, licenses, etc. Payments are usually done via consulting firms or in cash.
10. Kickbacks to state officials for keeping the business safe.



Case study 2: Pandora's box

TOP 5 International engineering company
Offices in Moscow, St. Petersburg and Sochi
Compliance investigation was launched after the claim received through a whistleblowing hotline

Initial findings:

- Corruption scheme involving the Company, Subcontractors and the Client;
- Serious FCPA violation;
- Top management's awareness about corruption issues;
- The Company manages 3 construction projects with total budget over $400M;
- Compliance policies are in place, but considered as less important than revenue.

Case study 2: Pandora's box

1. **Tender process manipulation**
2. **Subcontracting affiliated companies**
3. **Cashing out money via shell-companies**
4. **Facilitation payments to government officials for approvals of technical documentation**
5. **Payments for not-provided services**

Done:

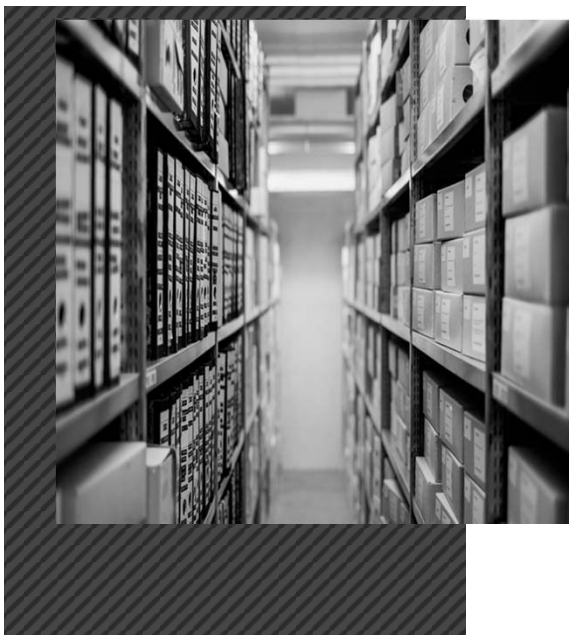
- Simultaneous visit to 3 offices;
- Over 30 devices collected and imaged;
- Over 20,000 paper documents digitized and uploaded to E-Discovery Platform;
- Over 2 Tb of information analyzed and…

Results of Investigation:

- 5 NEW Fraud schemes were identified and proved;
- 23 legal entities involved;
- Confirmation of management's intent and participation in fraud;
- USD 9.5 Mln withdrawn and distributed;
- Local management dismissal;
- Relaunch of compliance infrastructure.

Investigation steps

1 **Preliminary information review**	2 **Data collection and analysis**	3 **Decision making**	4 **Legal proceedings**
			HR proceedings
			PR proceedings
			Internal policies update
What is available for research and analysis? Who does what? Who knows whom? Possible difficulties	Accounting/ IDD / Interviews / eDiscovery	Decision on appropriate further steps to protect company's interests and mitigate possible risks	



Step 1. Preliminary analysis

Before going on-site you need to analyze what info may be requested, who could be your source, what are the possible pitfalls?

What is normally available?

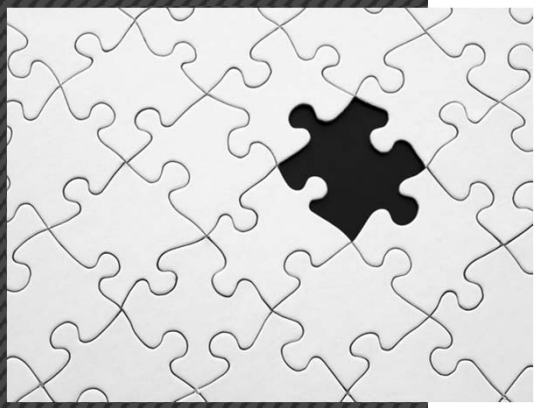
- Accounting records;
- Corporate policies and procedures;
- Corporate e-communication details (emails, Skype etc);
- Information on corporate business trips of suspects;
- Corporate mobile billing information;
- Information from employees;
- Other.

Step 1. Preliminary analysis

Before going on-site you need to analyze what info may be requested, who could be your source, what are the possible pitfalls?

Who does what? Who knows / covers whom?

- The compliance manager position can be concurrent, nominal or absent at all.
- Pay attention to family ties and informal relationship at the company.
- Check in advance what employees and business partners tell about the company in public.
- Collect info on who are business process owners and decision makers.
- Be attentive to any rumors about ties with state officials.



Step 1. Preliminary analysis

Possible difficulties: CIS specifics

- Accounting records are often segmental and can be just partially available in ERP system;
- Lot of paper work!
- Employees often use their personal electronic devices for business needs – check if BYOD policy is in place.
- Employees hardly believe in power and independence of compliance investigators.
- Police and other authorities can be used as instrument of influence against compliance investigators.
- Business interests prevail on compliance.
- Electronic devices can really be a treasury!

Step 2.1: Internal data collection and analysis

Data analytics to identify suspicious transactions

- Enrichment of accounting data with IDD scoring, electronic document approval logs
- Forensic tests (round sums, payments to shell companies, payments after hours, payments to companies where the client is a major source of revenue, salary and bonuses to non citizens, payments abroad, payments to “universal” vendors, split payments to sum below approval level, discounts to clients, etc.)
- Fraud scheme profiling based on identified cases

Analysis of documents

- Acts of acceptance
- Signatures
- Factual delivery of goods and services
- Technical and project documentation

Data collection

Goal:

Collect relevant information in the most effective manner

Major Data Sources

- Financial and contractual data
  - Export accounting data (1C, SAP, Oracle)
  - Export bank transactions (corporate internet banking application)
  - Contracts and supporting documents (invoices, acts of acceptance, etc.)
- Electronically Stored Information
  - Corporate computers
    - Email server
    - File server
    - Removable media
    - Smartphones
    - Backups
    - Business applications
    - Calls records
    - CCTV records
    - Access control system logs

Evidence stored on corporate devices

Information about real estate

Information about affiliated and involved parties

Information about corporate assets withdrawal

Financial and investment reports

Instructions and orders

Contracts, Invoices, Acts of acceptance

Payment orders, receipts

Travel and expenses information

Data collection pitfalls

- Custodians delete data, which may compromise them
- Company has shadow IT infrastructure on remote servers, where black accounting and other traces of illegal activity are stored
- Custodians are on the payroll of another company, IT-equipment belongs to another one legal entity
- Unauthorized changes in accounting databases
- Custodians hide removable media with related information
- Custodians steal computers, hard drives, servers
- Outsourced accounting system and hardcopy documents storage
- Custodians use personal devices for business tasks
- Encrypted or password protected data
- Destruction of documents' hardcopies

PLEASE NOTE!:
Accessing the sensitive data

Goal:
Collection and analysis of information meeting local and international data protection regulations

Common types of protected information:

- Personal data
- Private life and communications secrecy
- Bank secrets
- Corporate secrets
- Government secrets
- Tax secrets

Legal framework:

- 15 Federal laws in Russia+tens of other documents

PLEASE NOTE!:
Accessing the sensitive data

Corporate information policy:

- Company owns all data stored on corporate devices and IT-systems
- Company prohibits usage of corporate IT-infrastructure and assets in personal purposes
- Company may control the usage of corporate's assets by employees

Personal consent:

- Custodian allows the Company, Lawyers, Forensic provider to access, process and store PII and other information, including correspondence, stored on devices and in information systems
- Custodian allows to transfer PII abroad (if necessary)
- The aim of data collection and processing – perform-ance the review of business processes and operations, conduction of compliance review.

Contract with confidentiality and data protection clauses

Step 2.2. Integrity Due Diligence

Goal:
Collection of all available information from public and industry sources in the respective jurisdictions

Open sources enhanced review

- Corporate information databases :
  - Local: Lursoft, SPARK, Integrum, etc.;
  - International: Dun & Bradstreet, Orbis, Lexis Nexis, etc.
- Local and international corporate registries: tax authorities; ministry of justice, ministry of economy, etc.;
- Corporate disclosure web-portals: IFC.org; e-disclosure.ru; Bloomberg; Thomson Reuters;
- Other e-disclosure platforms: e.g. Offshore Leaks, Panama Papers;

Step 2.2 Integrity Due Diligence

Goal:
Collection of all available information from public and industry sources in the respective jurisdictions

Open sources enhanced review

- Media archives: Factiva, Integrum etc.;
- Social and professional networks: Facebook, Google+, LinkedIn etc.;
- Local and international litigation platforms: LexisNexis, Pravo.ru and others;
- Domain information sources: whois.net, whois.icann.org etc.;
- Local and international watch-lists: World-Check, C6, respective sources of state authorities.

Step 2.2 Integrity Due Diligence

Goal:
Collection of all available information from public and industry sources in the respective jurisdictions

Industry sources approach

- Current and former employees;
- Competitors;
- Market experts and analysts;
- Detectives;
- Former authorities' representatives.

Step 2.2 Integrity Due Diligence

Goal:
Collection of all available information from public and industry sources in the respective jurisdictions

What can be found on legal entities

- Corporate information:
  - Registration data;
  - Beneficial ownership structure;
  - Information on affiliated parties (both direct and indirect);
  - Financial information.
- Information on asset withdrawal schemes;
- Information on the target entity's assets owned in foreign jurisdictions;
- Information on the target entity's assets disputed in local or foreign jurisdictions;
- Affiliations with top management;
- Affiliations with state officials and government authorities;
- **Sanctions!**
- Other issues.

Step 2.2 Integrity Due Diligence

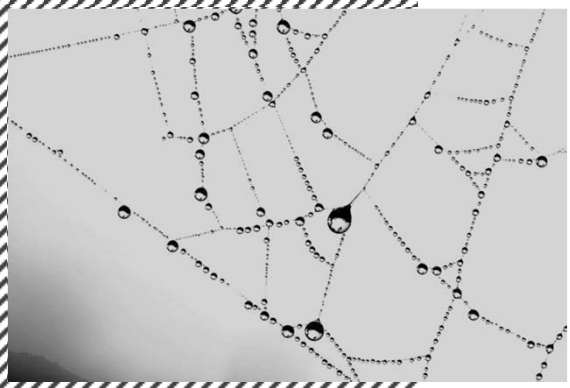
Goal:
Collection of all available information from public and industry sources in the respective jurisdictions

What can be found on subject individuals*

- Legal entities owned directly and through affiliated parties locally and abroad the country of residence;
- Real estate owned locally and abroad;
- Luxury items;
- Major investments and business interests;
- Habits and business 'modus operandi';
- Information on friends and relatives;
- Ties with state officials and government authorities;
- Allegations of fraud or wrongdoing;
- Other adverse issues.

* - subject to personal data protection restrictions

Step 2.3 Mass screening and cross affiliation check



Goal:
Risk assessment of counterparties.
Identification of connections between counterparties as well as employees and counterparties.

Availability of data

- Publicly available sources in Russia, Ukraine and Kazakhstan provide extensive information about local companies.
- Information from these sources can be used for automated screening of multiple companies (up to several thousands).
- Mass screening is performed using a tailored risk model. The model can be adjusted based on business requirements.

Step 2.3 Mass screening and cross affiliation check

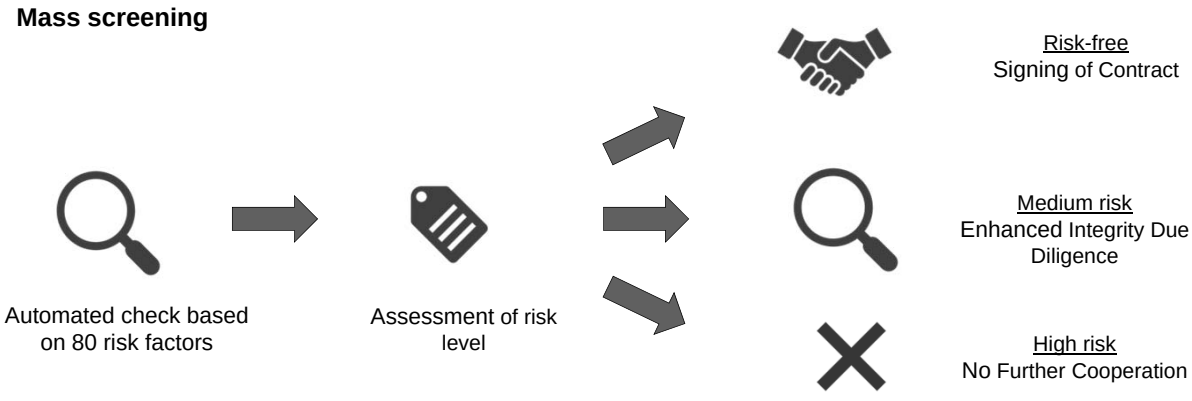
Goal:
Risk assessment of counterparties.
Identification of connections between counterparties as well as employees and counterparties.

What do we get

- Risk assessment: each counterparty is granted with particular risk rating: high, medium and risk-free. Company can make decision based on these ratings.
- Conflict of interest check: affiliations between employees and counterparties.
- Unfair tenders: affiliated counterparties participating in the same tender.
- Price collusion: several counterparties, instructed by the company's dodgy management, provide unfair prices.
- Affiliation with Sanctioned subjects / state officials.

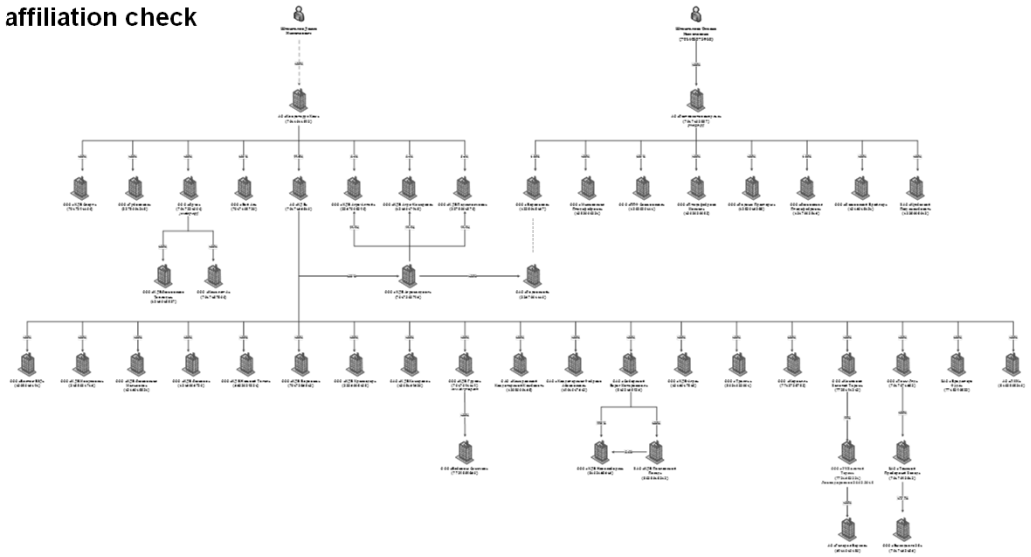
Step 2.3 Mass screening and cross affiliation check

Mass screening



Step 2.3 Mass screening and cross affiliation check

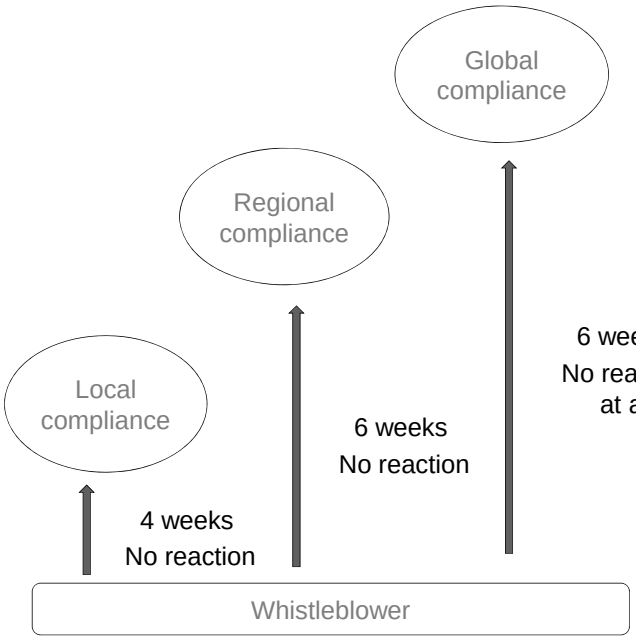
Cross affiliation check



STEP 3. Decision making

- Understanding of real situation
- Dismissal of involved employees
- Damages recovery
- Legal proceedings
- Reputation recovery

Case study 3:
Pick-up the phone



World TOP 3 industrial company
15,000 employees received an email from a whistleblower with negative info against its local management and the company's compliance

Key findings:

- The whistleblower tried to approach the company's compliance several times – no results;
- Every time the compliance officers reported the matter to the top management they were ignored;
- Approaching the next level of communication the individual added negative info on those who did not react before;
- In the end, patience is over.

Step 4.1 Legal proceedings

Goal:
Asset recovery, transferring the responsibility on involved individuals and companies

Three major ways to moving forward

- Pre-litigation proceedings (asset freeze, negotiation, settlement);
- Local litigation (both commercial and criminal);
- International litigation (both commercial and criminal).

Step 4.1 Legal proceedings

Things to keep in mind

- Compliance with local laws is always a priority in CIS
- Police is not interested in investigating your case. At all.
- You need local lawyers to handle a case either in court or in police.
- Full report with investigation results + properly collected evidence provided with your claim to the police may increase probability of achieving the goal.
- Criminal prosecution may be used to obtain evidence for civil case.
- Criminal court decision helps to win civil case.
- Be ready to trace assets abroad and submit claims against the subjects's relatives and affiliated entities.
- Decisions of CIS courts and police can be questionable.
- Initiate several cases to pursue subject in different jurisdictions.

Step 4.2 HR Proceedings

Goal:
Arrange dismissal of the employee involved in wrongdoing on best terms for the company

Attention to documents!

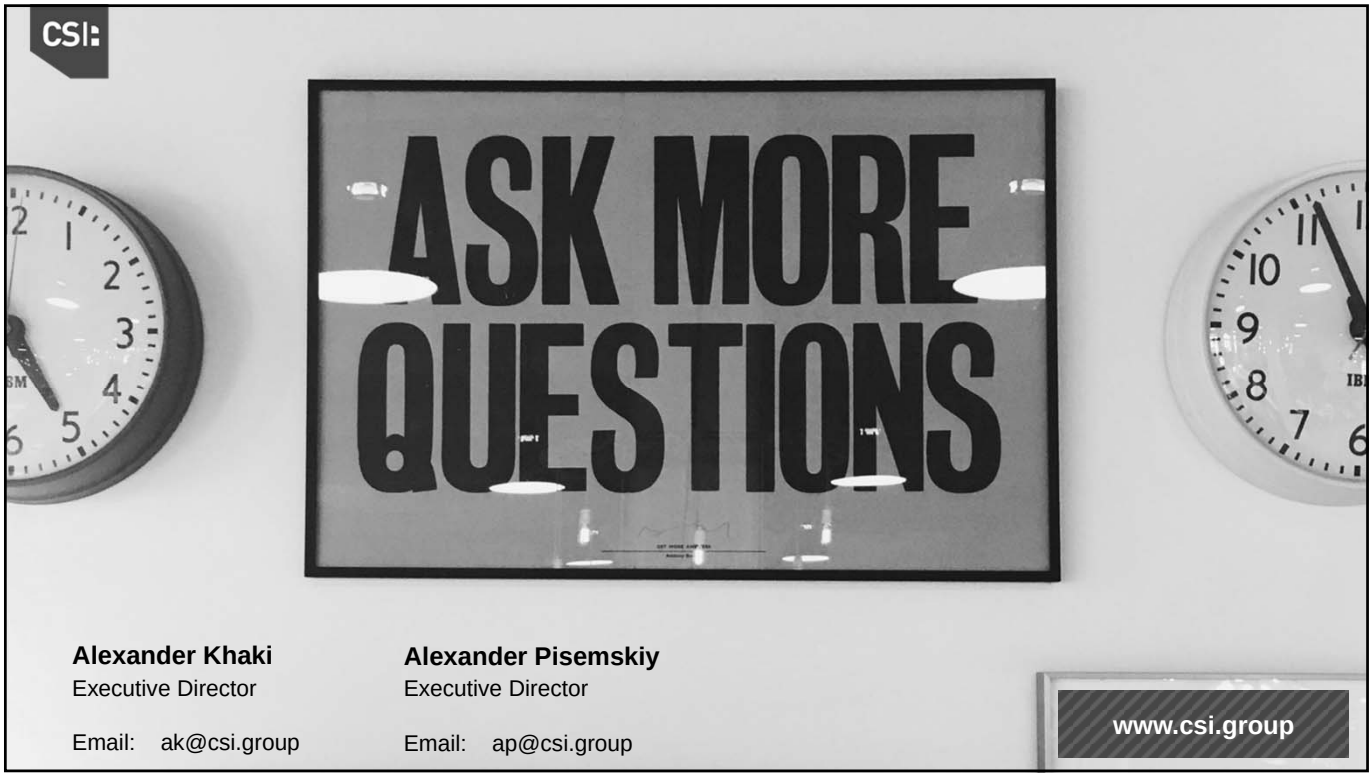
- CEO's order to investigate the issue
- Data collection and analysis records
- Investigation report with clear evidence of the subject's violations of policies and laws
- Legal opinion on dismissal reason
- Notification to employee about the investigation results and clarifications from him/her

Be ready to provide all documents to the court!

Step 4.3 PR proceedings

Chance to demonstrate zero tolerance to fraud

- Tell the market your version of the story before it will be done by a counter party.
- Declare and promote your values and ethical behavior.
- Demonstrate your readiness to pursue individuals violating policies and laws, including law enforcement.
- PR support works perfectly to counter usage of ”administrative resource” by counter party.
- Publicly available information about wrongdoings performed by individual will help to question source of income and freeze assets abroad.
- Use SEO to promote posts and information supporting your position.



Alexander Khaki
Executive Director
Email: ak@csi.group

Alexander Pisemskiy
Executive Director
Email: ap@csi.group

www.csi.group