Kazakhstan Economic Crime Survey 2016

35%

of respondents have experienced an economic crime in the last 24 months

91%

of respondents believe vendor selection to be the procurement stage most susceptible to fraud

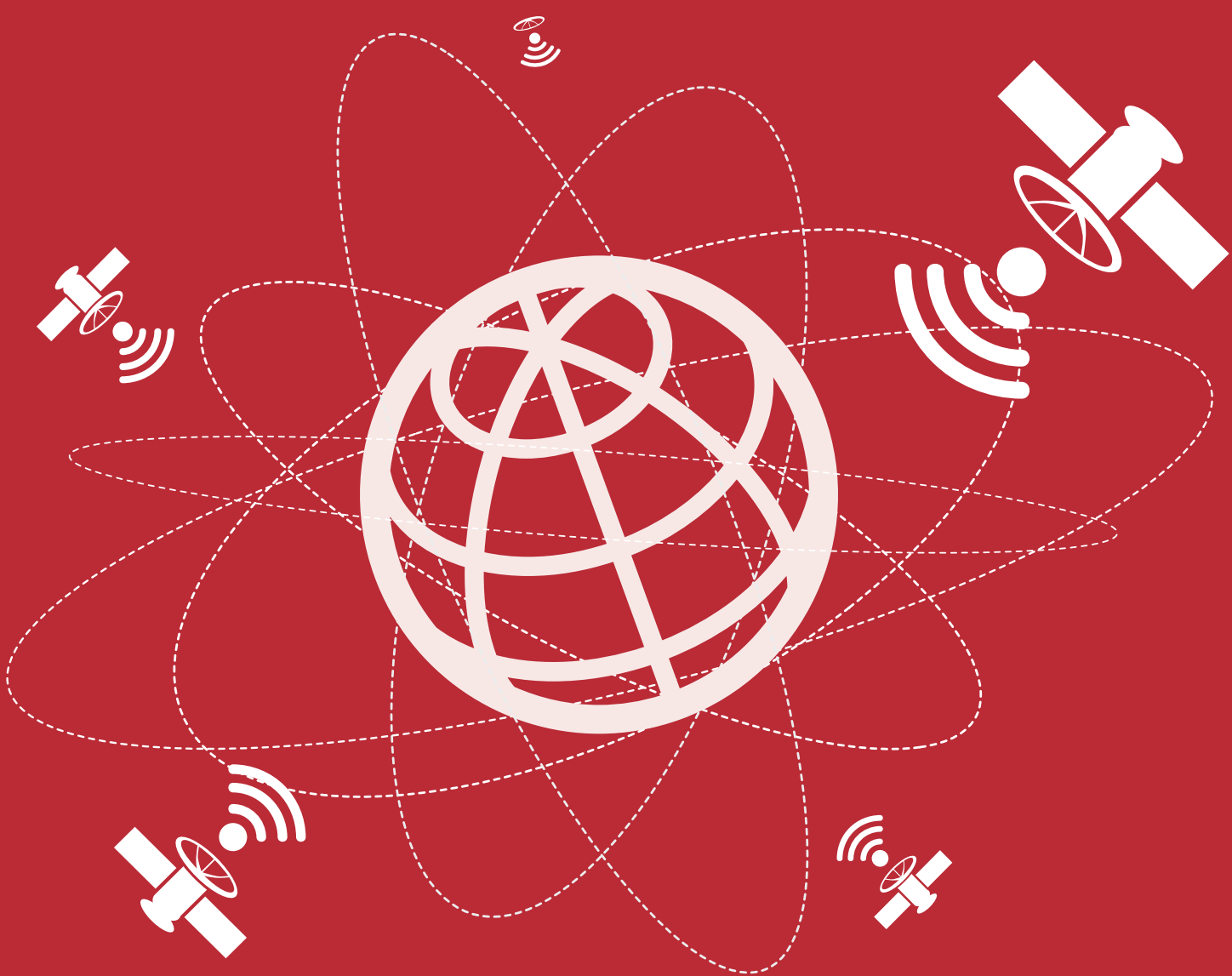
36%

of organisations surveyed have never performed a risk assessment

pwc

www.pwc.kz

Contents



Foreword

PwC has been publishing its Global Economic Crime Survey since 1999. This biennial survey has been one of the premier thought leadership publications on economic crime.
As economic crime is of particular concern for business and government leaders in Kazakhstan, we thought it would be helpful to present a separate survey for the country and start building the supporting foundation for actions taken by these leaders in combating fraud.

Hence, we are very pleased to present the results of the 2016 Economic Crime Survey in Kazakhstan.

The Survey outlines the current situation with fraud risks in organisations across the country and allows comparing Kazakhstan to the rest of the world.

We are very grateful to the participants of this survey who have provided us with insightful information on the current and anticipated economic crime challenges, and responses. We believe the Survey will help leaders better assess risks and prepare for mitigating the fraud risks in their organisations.

Konstantin Yeliseyev
Partner,
Eurasia Deals Leader

Highlights of the survey

- In Kazakhstan, 35% of organisations have experienced an economic crime in the last 24 months, which is on par with the global survey results (36%).
- Fraud is considered a significant future threat. For instance, 40% of respondents in Kazakhstan, and 36% of global respondents, believe that it is likely that their organisations will experience economic crime over the next two years.
- In Kazakhstan, 30% of respondents reported a loss of less than USD 100,000 due to economic crime in the past 24 months, while 25% experienced losses between USD 100,000 and USD 1 million. Furthermore, 34% of respondents have experienced losses in excess of USD 1 million. In addition to financial losses, every economic crime results in collateral damage.
- Overall, 52% of organisations, which have suffered economic crime in Kazakhstan in the last 24 months, stated that this has had a negative effect on employee morale. Globally, 44% of respondents also stressed this negative impact on employee morale.
- Amongst those who have suffered economic crime over the last two years, asset misappropriation was highlighted as the main type of fraud (cited by approximately 63% of respondents in Kazakhstan, and 64% globally). Asset misappropriation has traditionally been regarded as one of the easiest types of fraud to detect, thus its prevalence in our survey is not unexpected.
- Our survey shows that asset misappropriation is followed by procurement fraud. The number of responses related to procurement fraud is higher in Kazakhstan (46%) than the global result (23%). The process of vendor selection is stated by Survey respondents to be the most vulnerable area of the procurement process (91%).
- Bribery and corruption are regarded as the next most common type of economic crime in Kazakhstan. For instance, 38% of respondents were affected by bribery and corruption in Kazakhstan in the last two years compared to 24% globally.
- Only 4% of respondents in Kazakhstan were aware of their organisations having experienced cybercrime in the last two years, in contrast to 32% of

- respondents globally. Furthermore, 17% of respondents in Kazakhstan and 34% of those surveyed globally believe that their organisation will be threatened by some type of corporate cybercrime in the next 24 months.
- There are many causes of economic crime. Fraud experts often point to the three factors that may be detected when fraud occurs (referred to as the “Fraud Triangle”): 1) opportunity or ability to commit a crime; 2) incentive or pressure; and 3) rationalisation for such a crime. Respondents in Kazakhstan believe that opportunity or ability to commit a crime is the most important factor (80%), while globally opportunity or ability to commit a crime is also cited as a key factor (69%).
- Assessment of fraud risks is an essential tool for identifying such threats as weaknesses in controls, which, in turn, lead to opportunities to commit fraud. Globally, 51% of respondents tend to perform risk assessments at least annually, while in Kazakhstan, only 32% of respondents confirmed that their organisations conduct a fraud risk assessment at least once a year. It is worth noting that 36% of respondents in Kazakhstan indicated that their organisations have never performed fraud risk assessments.
- Both in Kazakhstan (63%) and globally (46%), respondents believe that internal actors are the most common perpetrators of economic crime. In particular, respondents in Kazakhstan described a typical internal fraudster's profile as a senior manager (53%), who is 31 to 40 years old (50%), male (79%), with three to five years of service in the company (50%), and holding a university/college degree (86%).
- In the majority of cases, internal perpetrators in Kazakhstan and globally were dismissed (in 67% and 76% of cases, respectively).
- In cases where an economic crime involves a third party, organisations in Kazakhstan prefer to take civil action (67%) and terminate business relationships (67%), while globally companies prefer to inform law enforcement (53%).

Economic crime trends

Incidents of economic crime

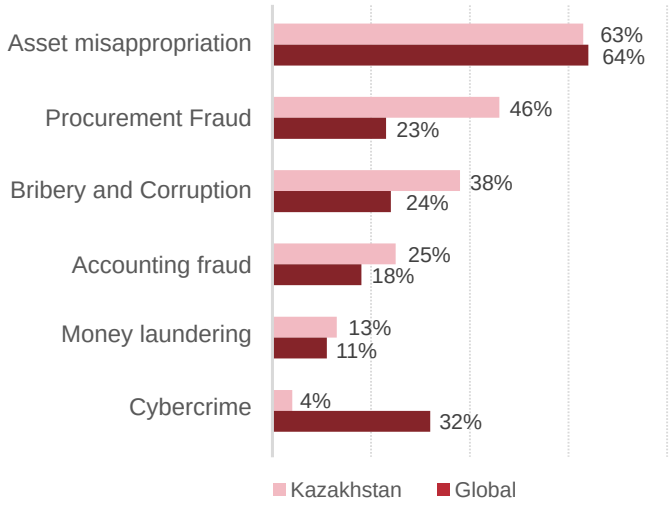
In Kazakhstan, 35% of respondents reported that they have experienced an economic crime in the last 24 months. This rate is very close to the global result (36%).

However, 22% of respondents are not certain (compared to 11% globally) as to whether or not they have been victim of fraud. Potentially, this group may have a significant impact on economic crime statistics in the future.

Types of economic crime

The most common economic crimes reported by our respondents in 2016 are presented below.

Fig 1: Main types of economic crime in Kazakhstan compared to global trends



Asset misappropriation is viewed as the most common form of economic crime, both in Kazakhstan and globally. For instance, 63% of our respondents in Kazakhstan and 64% of our respondents globally reported being victims of such misappropriation. The prevalence of asset misappropriation among other types of economic crime is not surprising. Typically, asset misappropriation is easier to detect, since this type of fraud is not as complicated as, for example, bribery, corruption or cybercrime.

Procurement fraud was commonly cited (46%), making it the second most frequently reported type of fraud in Kazakhstan. The indicator is twice as high as the global average (23%).

The number of responses related to bribery and corruption was notably higher in Kazakhstan (38%) than the global average (24%).

The number of responses related to accounting fraud was higher in Kazakhstan (25%) than the global average (18%).

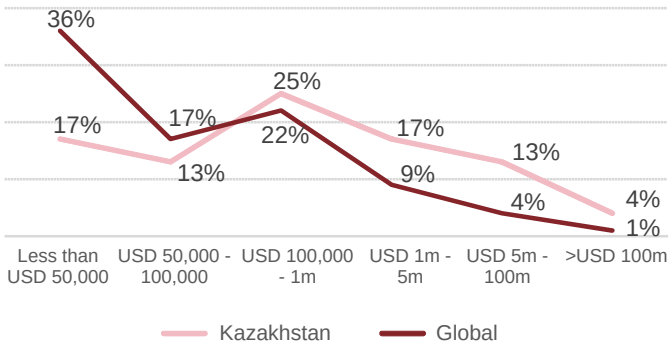
At the same time, the total number of responses citing cybercrime is significantly lower in Kazakhstan (4%) than reported globally (32%). Does this mean that Kazakh business is less exposed to cybercrime? In this respect, we should remember that a significant percentage of those who did not report cybercrime could have suffered an incident, but may not even have known about it.

Negative consequences of economic crime

When an economic crime occurs, one of the key questions for an organisation is the size of the loss it must bear. In Kazakhstan, 30% of respondents who have experienced economic crime reported losses under USD 100,000 and this is lower than the results given globally (53%). At the same time, 25% of respondents lost between USD 100,000 and USD 1 million (22% globally). In Kazakhstan, 34% of respondents reported losses in excess of USD 1 million while, globally, only 14% of those surveyed had experienced such significant damage.

In general, the true cost of economic crimes is difficult to estimate, since reported financial losses often appear as small components of larger, more serious issues.

Fig 2: Financial loss from economic crimes



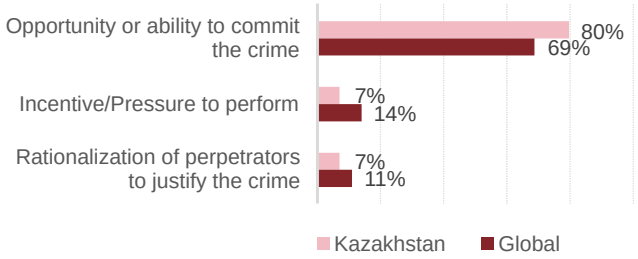
We believe it is important not to ignore the collateral damage from fraud, such as employee morale (52%), damage to company's business relations (50%) and company's relations with regulators (46%) which were all reported by respondents in Kazakhstan as the most significant non-financial losses or "side effects" from economic crimes. The negative effect of economic crime on employee morale might be the result of expanding transparency in the business community coupled with declining tolerance towards corrupt behaviours.

Fig 3: Negative consequnces (high and medium impact) suffered due to economic crime

Causes of economic crime

Academic research shows that usually there are three factors that stand behind any fraud activity (the aforementioned "Fraud Triangle"). Firstly, a perpetrator of fraud needs an incentive or pressure to engage in misconduct. Secondly, there should be an opportunity to commit a fraud. Lastly, a basis for rationalisation or justification of a perpetrator's actions can also play a key role. Our survey indicates that opportunity to commit a crime is perceived by respondents in Kazakhstan as a major factor behind fraudulent activities (80%), while globally this is also a major factor (69%).

Fig 4: Factors contributing to economic crime commited by internal perpetrators



Fraud detection and investigation

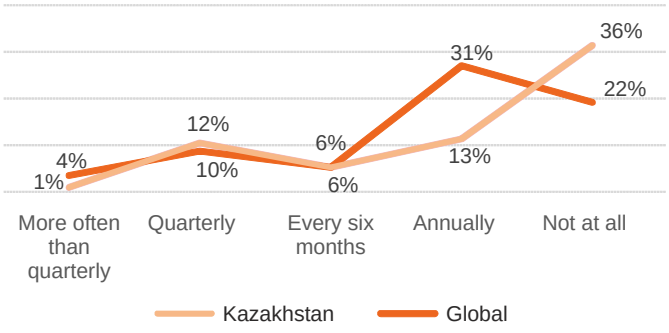
Risk assessments

Fraud risk assessment is essential for identifying threats and weaknesses in corporate controls that, in turn, give rise to opportunities to commit fraud.

In Kazakhstan, the number of respondents who reported that regular risk assessments are performed within their organisations is lower than the global response (32% vs 51%). In addition, the number of companies that have never performed a risk assessment in Kazakhstan is higher than the global average (36% vs 22%).

As mentioned above, respondents both in Kazakhstan and around the world consider the opportunity or ability to commit fraud to be the most important factor contributing to the occurrence of such crimes. Thus, it is even more vital that companies conduct risk assessments, as they can help identify internal control weaknesses and prevent, or at least mitigate, the risk of economic crime.

Fig 5: Minimum frequency of performance of fraud assessments



Effective fraud risk assessment should:

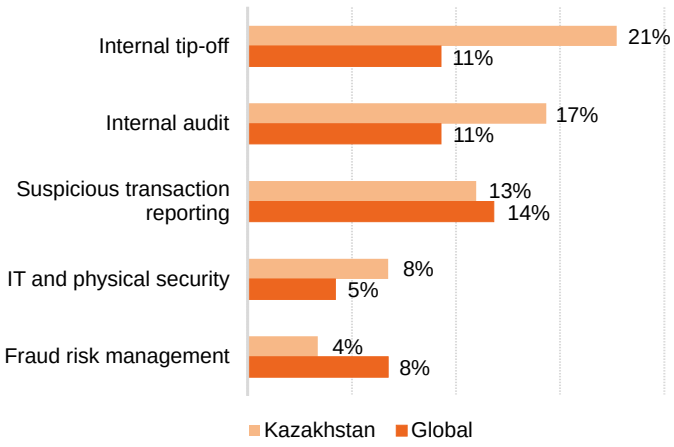
- identify potential inherent fraud risks;
- determine people and departments that are more likely to commit fraud and identify the methods likely to be used;
- identify and map existing preventive and investigative controls for relevant fraud risks;
- evaluate whether the relevant controls and processes are effectively designed to address identified fraud risks;
- identify and evaluate residual fraud risks resulting from ineffective controls.

Detection of economic crimes

Our survey shows that the majority of economic crimes in Kazakhstan were initially detected by internal tip-offs (21%) and internal audit functions (17%). The global results differ, at 11% and 11%, respectively.

Globally, the leading method for detecting economic crime is reporting on suspicious transactions (14%), which is similar to the result for Kazakhstan (13%).

Fig 6: Fraud detection methods in Kazakhstan and globally



Investigation

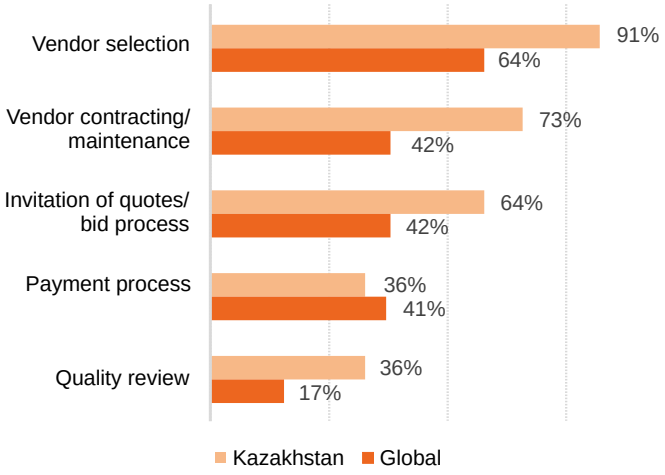
When an incident of potential fraud is identified, in most cases (68%), respondents stated that they relied on their internal resources to perform investigations and this is in line with the global trend (72%). However, it should be noted that 28% of respondents in Kazakhstan reported engaging a specialist forensic investigator in cases fraud had been uncovered, which is higher than the global result (20%).

Fig 7: Fraud investigation methods in Kazakhstan and globally

Procurement fraud

Our survey shows that vendor selection is the most vulnerable area of procurement in Kazakhstan (91%). Vendor contracting/maintenance is the second area that is most susceptible to procurement fraud in the country (73%). We believe that fraud in procurement can be averted by strengthening controls within buyers themselves through due diligence and internal monitoring of the contracting process.

Fig 8: Areas of procurement fraud



Bribery and corruption

The survey shows that 38% of respondents in Kazakhstan have experienced bribery and corruption in the last two years and this is higher than the global average (24%).

For instance, 16% of respondents admitted that their organisations had been asked to pay a bribe, while 25% of them believe that they lost an opportunity to a competitor that paid a bribe.

Bribes can take many forms, including money (or cash equivalent such as shares), unreasonable gifts, entertainment or hospitality, kickbacks, unwarranted rebates or excessive commissions (e.g., paid to sales or marketing agents), “facilitation” payments/payments made to certain parties so that they perform their normal job more quickly and/or prioritise a particular customer and political/charitable contributions.

Kazakhstan recently adopted various anti-corruption regulations and laws.

Furthermore, the Government of Kazakhstan, with the support of the Organisation for Economic Co-operation and Development (OECD), has been undertaking intensive efforts to tackle corruption in the country.

For instance, the Istanbul Anti-Corruption Action Plan (IAP), adopted in 2003, is a sub-regional initiative of the OECD Anti-Corruption Network for Eastern Europe and Central Asia (ACN). It targets such countries as Azerbaijan, Armenia, Georgia, Kazakhstan, Kyrgyzstan, Mongolia, Tajikistan, Ukraine and Uzbekistan. Other ACN countries are also taking part in the plan. The IAP involves systematic and regular peer reviews of legal and institutional frameworks for fighting corruption in the targeted countries.

On 10 October 2014, the OECD prepared Kazakhstan for the third round of monitoring under the IAP. The report produced provides an analysis of the progress achieved by Kazakhstan in its anti-corruption reforms, as well as the status of recommendations presented to the country during its second round of monitoring in September 2011. In particular, the third round report contains new recommendations with respect to anti-corruption policies and criminal liability for corruption. Fighting corruption remains a policy priority in Kazakhstan, as reflected in statements made by the highest officials of the OECD.

Anti-corruption procedures have already been enshrined in a number of key official documents, including the President's Annual Address, and the Strategic Development Plan of Kazakhstan for the period until 2020, etc.

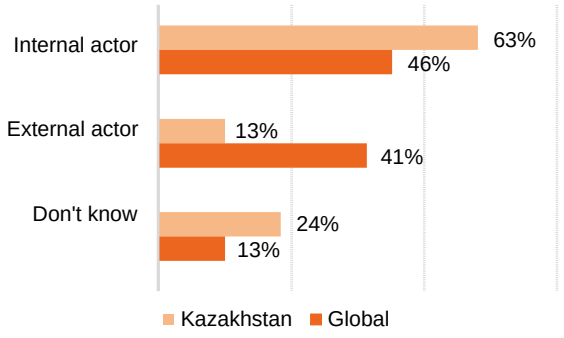
External or internal perpetrators

In Kazakhstan, 63% of respondents state that the main perpetrators of their fraud incidents were employees. This may be partially owing to the fact that organisations have better security for external threats rather than internal.

External perpetrators were reported by only 13% of the respondents, which is significantly lower than what was reported globally (41%).

However, 24% of respondents could not provide a definitive answer and this group might further affect the actual proportion of internal and external perpetrators.

Fig 9: Perpetrators of fraud

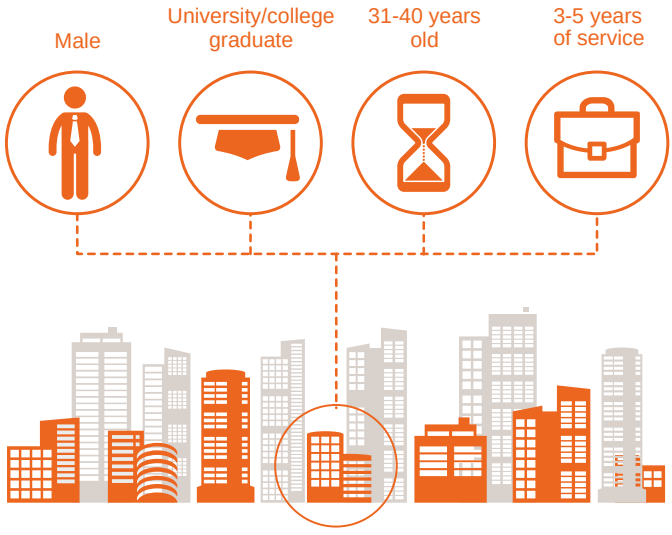


Profile of an internal fraudster

Both in Kazakhstan and globally, economic crimes are largely committed by internal perpetrators. In Kazakhstan, 53% of respondents believe that a typical internal fraudster belongs to senior management. Only 16% of respondents globally believe that senior management are the main culprits in this regard.

In Kazakhstan, the majority of fraudsters were male (79%), from 31 to 40 years old (50%), with a university/college degree and who had joined the company within the past three to five years.

Most likely characteristics of the internal fraudster



Profile of an external fraudster

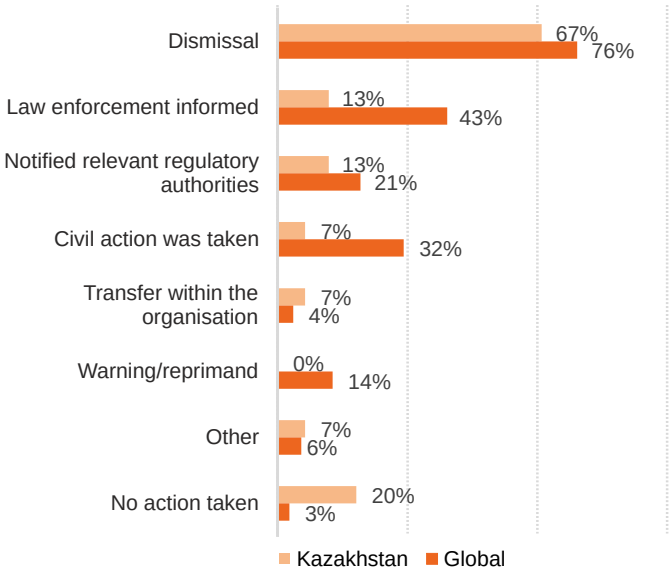
The main perpetrators of external fraud reported by respondents in Kazakhstan were customers (67%) and suppliers (33%). This was, in fact, higher than the results reported globally (25% and 10%, respectively).

We believe that the common types of customer fraud are likely to be schemes related to receiving commercial bribes (i.e. money paid by customers to sales managers in order to receive favourable terms) and giving commercial bribes (i.e. money paid to customers to retain business).

Combatting internal and external perpetrators

In the majority of cases, internal perpetrators in Kazakhstan were dismissed (67%). At the global level, dismissal is also the most frequent way of dealing with an internal perpetrator (76%).

Fig 10: Actions taken by organisations against internal perpetrators



In those cases where economic crime involved a third party, organisations in Kazakhstan preferred to take civil action (67%) and/or terminate a business relationship (67%), while globally, organisations prefer to inform law enforcement (33%).

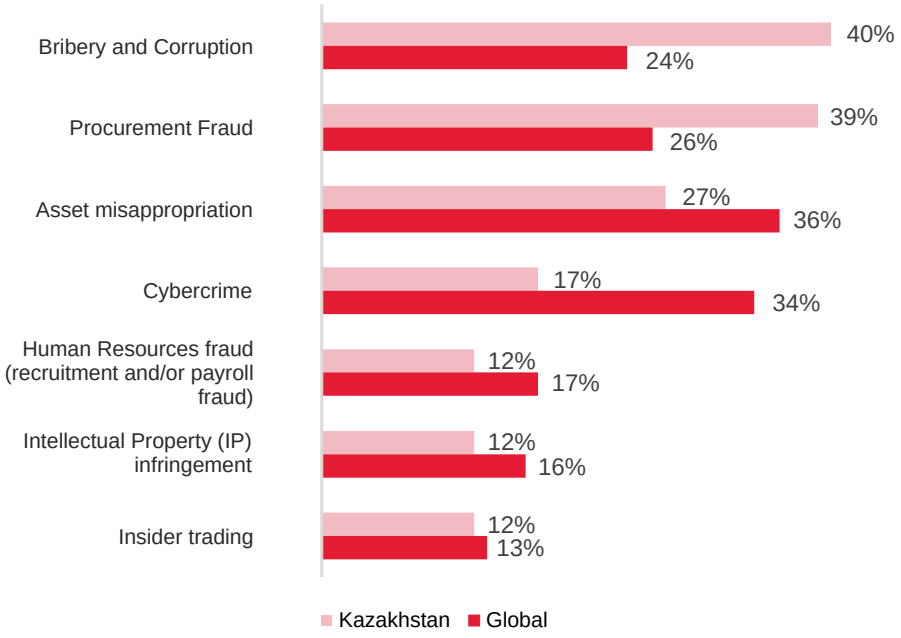
Fig 11: Actions taken by organisations against external perpetrators

Fraud horizon

Fraud is viewed as a future threat with many respondents believing that their organisations will experience economic crimes in the next 24 months.

In Kazakhstan, 40% of respondents believe that their organisations will experience cases of bribery and corruption in the next 24 months compared to 24% globally.

Fig 12: Main types of expected economic crimes in Kazakhstan and globally



At the same time, 39% of respondents believe that they are likely to experience procurement fraud in the next 24 months compared to 26% globally.

Among global respondents, asset misappropriation and cybercrime are the most likely types of crime (36% and 34%, respectively).


OUR APPROACH... to accelerate benefits
DEPLOYMENT
SUSTAINABILITY
CHANGE MANAGEMENT
GOVERNANCE
FIT FOR PURPOSE SOLUTIO
W WE ENSURE SUSTAINABLE CHANGE

Terminology

Due to the diverse descriptions of individual types of economic crime in the legal statutes of different countries, we have developed the following categories for the purposes of this survey. These descriptions were defined as such in our web survey questionnaire.

Accounting fraud

When financial statements and/or other documents are altered or presented in such a way so that they do not reflect the true value or financial activities of an organisation. This can involve accounting manipulations, fraudulent borrowings/raising of finance, fraudulent application for credit and unauthorised transactions/rogue trading.

Asset misappropriation, including embezzlement/ deception by employees

The theft of assets (e.g., monetary assets/cash or supplies and equipment) by directors, persons in fiduciary positions or other employees for their own benefit.

Bribery

The unlawful use of an official position to gain an advantage in contravention of duty. This can involve the promise of an economic benefit or other favour, as well as the use of intimidation or blackmail. It can also refer to the acceptance of such inducements. Specific examples include kickbacks, extortion, gifts (with strings attached), facilitation payments, etc.

Corruption

Dishonest or fraudulent conduct by those in power, typically involving bribery.

Cybercrime

Also known as computer crime, cybercrime is an economic offence committed using a computer and/ or Internet. Typical instances are the distribution of viruses, illegal downloads of media, phishing & pharming, and theft of personal information (e.g. bank account details). This excludes routine fraud, whereby a computer is used as a byproduct in order to carry out a fraud, and only includes such economic crimes where a computer, Internet or use of electronic media and devices is the main element and not simply incidental.

Economic crime

The intentional use of deceit to deprive another of money, property or a legal right.

Financial loss

When estimating financial losses due to fraud, participants should include both direct and indirect losses. Direct losses are the actual size of the fraud in question, while indirect losses would typically include the costs involved with investigation and remediation of the problem, penalties levied by the regulatory authorities and litigation costs. This should exclude any amount estimated due to “loss of a business opportunity”.

Fraud risk assessments

Assessments are used to ascertain whether an organisation has undertaken initiatives to specifically consider:

a. the fraud risks to which its operations are exposed;

b. an assessment of the most threatening risks (i.e., evaluating risks for significance and likelihood of occurrence);

c. identification and evaluation of controls (if any) that are in place to mitigate key risks;

d. assessment of the general anti-fraud programmes and an organisation's control; and

e. actions to remedy any gaps in such controls.

Incentive/pressure to perform

When an individual has some financial problem that he/she is unable to solve through legitimate means, so he/she considers committing an illegal act as a way to solve the problem. The financial problem may be professional (e.g., job is in jeopardy) or personal (e.g., personal debt).

Intellectual property (IP) infringement

IP infringement covers trademarks, patents, counterfeit products and services. This includes the illegal copy and/or distribution of fake goods in breach of patent or copyright, as well as creation of false currency notes and coins with the intention of passing off as genuine.

Money laundering

Actions intended to legitimise the proceeds of crime by disguising their true origin.

Opportunity or ability

When an individual uncovers a way where he/she can use (abuse) his/her position of trust in order to solve a financial problem with a low perceived risk of getting caught.

Procurement fraud

Illegal conduct by which an offender gains an advantage, avoids an obligation or causes damage to his/her organisation. The offender might be an employee, owner, statutory board member, an official, a public figure or a vendor who was involved in the purchase of services, goods or assets for the affected organisation.

Rationalisation

When an individual finds a way to justify the crime to himself/herself in a way that makes it an acceptable or justifiable act.

Contacts

Survey leadership team

Konstantin Yeliseyev
PwC Kazakhstan | Partner
Office: +7 727 330 3200
Email: konstantin.yeliseyev@kz.pwc.com

Irina N Novikova
PwC Russia | Partner
Office: +7 495 232 5735
Email: irina.n.novikova@ru.pwc.com

Inna Fokina
PwC Russia| Partner
Office: +7 495 967 6382
Email: inna.fokina@ru.pwc.com

Natalia Gubareva
PwC Russia | Director
Office: +7 495 967 6338
Email: natalia.gubareva@ru.pwc.com

Tatiana Vostrova
PwC Russia | Director
Office: +7 495 223 5086
Email: tatiana.vostrova@ru.pwc.com

Alexander Dmitriev
PwC Russia | Director
Office: +7 495 223 5065
Email: alexander.dmitriev@ru.pwc.com

Vladimir Nefediev
PwC Russia | Director
Office: +7 495 232 5587
Email: vladimir.nefediev@ru.pwc.com

Survey management and methodology

Anton Ulyakin
PwC Russia | Manager
Office: +7 495 967 6000
Email: anton.ulyakin@ru.pwc.com

www.pwc.kz