

Russia

# Economic crime in a downturn

The 5th Global economic crime survey



# Content

## Introduction

We are pleased to present the results of the Economic crime survey in Russia. The survey was prepared based on the 5th Global economic crime survey data.

More than 3,000 respondents from 55 countries, including 86 representatives of Russian leading entities, took part in the 2009 Global economic crime survey. This year we have an opportunity to evaluate trends on fraud spanning a 10-year period.

The survey was designed to seek respondents views on economic crime in general and, specifically, on fraud in the downturn. We were particularly interested in finding out which changes took place in this area as a result of the economic downturn. Therefore, we asked respondents to tell us about fraud cases in their businesses in the last year during the period that roughly corresponded with the global financial crisis.

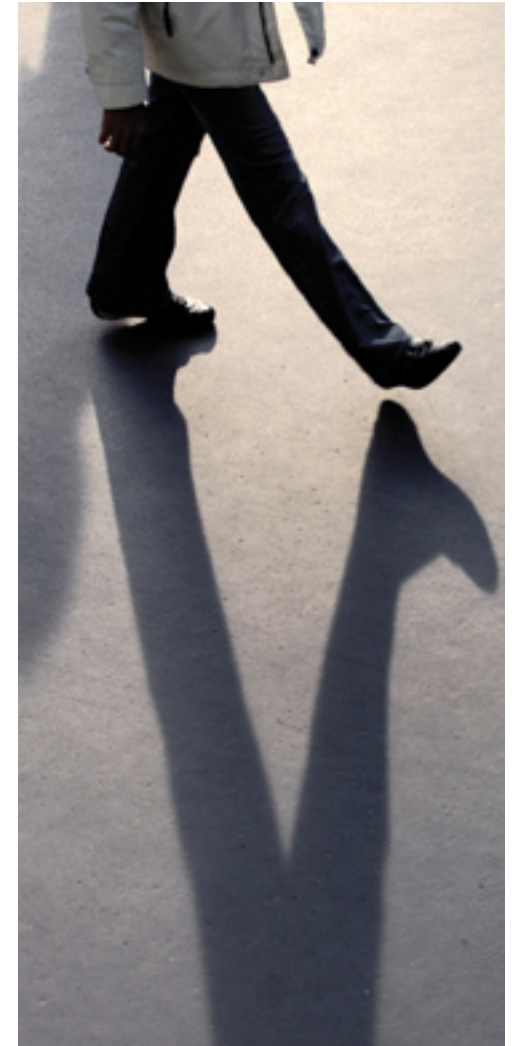
The INSEAD Business School in France assisted us in designing the questionnaire and data processing – this lent a certain amount of academic rigour to the report.

While preparing the report, we treated all replies in confidence. Information received in the course of this survey was used without referring to any specific entity and was only linked to the industry, company size and other demographic data.

Thanks to the data received from respondents, we obtained a comprehensive understanding of the entities' perception of commercial crime, their awareness about commercial crime and the impact of fraud on business.

This survey covered a good mix of companies, operating in Russia, that include private (51%), publicly listed (34%) and public sector companies (12%). Companies operating mainly in Russia made up 31% of the total number of respondents. Such sectors as financial services (26%), energy utilities and mining (15%), manufacturing (9%), automotive (8%) and pharmaceuticals (8%) are the most widely represented in the survey (see fig. 1).

According to the survey data, 57% of respondents work in organisations with 1,000 staff or more, and 36% of the survey respondents were executive officers or board members.



## Key findings

- Our survey reveals that fraud remains one of the most problematic risks for businesses worldwide.
- In Russia, 71% of organisations were victims in the last 12 months alone. This is a shocking 12 percentage points increase compared to our last Economic crime survey in 2007 (59%) and is well above the global (30%), Central and Eastern Europe (CEE) (34%) and BRIC<sup>1</sup> countries (34%) results.
- Nearly half (48%) of Russian companies surveyed reported an increase in the number of economic crime incidents over the last 12 months. Of those who have been the victim of economic crimes, 61% said they had experienced from one to 10 incidents, and 39% had suffered more than 10 instances.
- Roughly half (51%) of Russian companies surveyed believe that their organisation faces a greater risk of economic crime in the current economic situation.
- Increasing pressures and incentives to commit fraud due to the economic downturn are considered the most likely reason for an increased risk of fraud by 86% of Russian companies.
- Asset misappropriation remains the most common type of economic crime reported in Russia (64%), and bribery and corruption continue to be a major challenge in the Russian market – 48% of respondents were affected in the last year.
- A lowering of employee morale was cited by 44% of Russian companies as the most significant collateral damage caused by economic crimes in last 12 months.
- Some 62% of Russian companies believe that a party external to the company played a role in the fraud. Agents and intermediaries are a particular risk.
- Russian companies use criminal charges, civil complaints and the cessation of business relationships (56% each) as actions against external perpetrators, or, in the case of internal perpetrators, dismissal (57%).
- Nearly half (45%) of Russian companies expect to become the victim of asset misappropriation in the next 12 months. A high proportion, but overly optimistic given the actual incidence rate.



## Fraud – a clear and present danger

The Economic crime in a downturn survey reveals that 71% of Russian organisations report being subject

to one or more significant economic crimes in the last 12 months. This is a shocking 12 percentage points increase compared to our 2007 research (59%), and is well above the global (30%), Central and Eastern

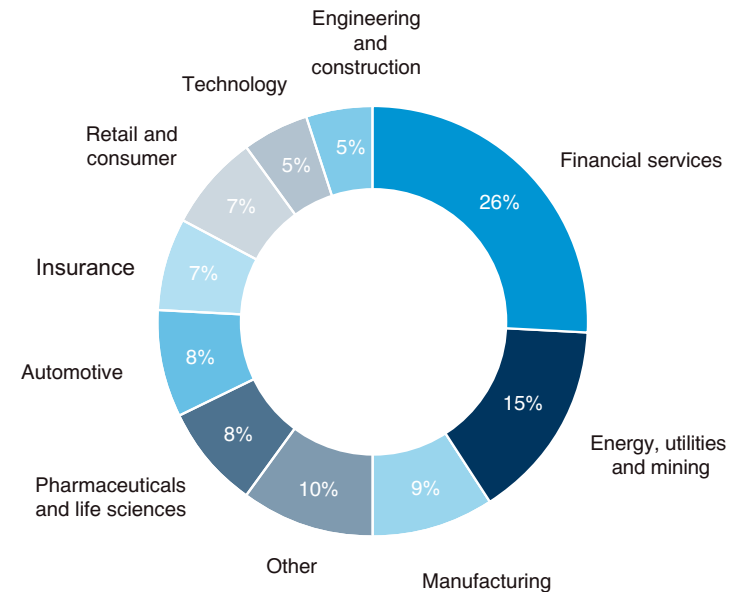
Europe (CEE) (34%) and BRIC<sup>2</sup> countries (34%) results.

This is clearly an issue that can't be overlooked by any organisation doing business, or planning to do business,

in Russia. As might be anticipated from the very high overall reported crime rate, all industries reported high incidence rates with no industry particularly spared.



Figure 1. Respondents by industry\*



\*% of all respondents

<sup>2</sup> For the purpose of this study BRIC group include Brazil, Russia, India, China, Indonesia, Mexico and Turkey.

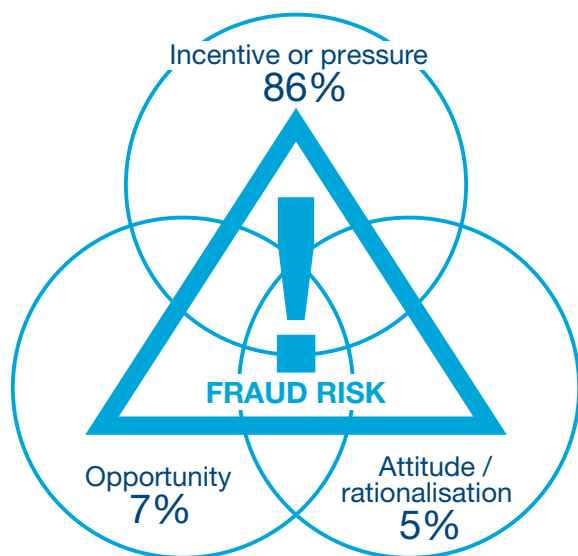
## Economic downturn and the heightened risks of fraud

The global economic downturn has significantly affected most organisations. 66% of respondents reported a decline in financial performance during the last 12 months. The current economic climate has equally affected organisations' view on fraud risks, with 51% of respondents reporting that they believe their organisation currently faces a greater risk of economic crime.

In response to a specific question, 48% of Russian companies reported

an increase in the number of economic crime incidents in the last year. Of the victims of economic crime, 61% said they had experienced from one to 10 incidents, and 39% had suffered more than 10 instances.

When economic survival is threatened (either for the organisation or for the individual), the line separating acceptable and unacceptable behaviour can, for some, become blurred. 98% believed that at least one of free factors of the fraud triangle had increased over the last year. However 86% citing heightened incentives or pressures to commit fraud.



**Figure 2. Reasons cited by companies to explain what has contributed to increasing pressure and incentives to commit fraud\***



\*% of respondents who cited incentive of pressure as a most likely reason for greater risk of fraud in the current economic environment

Respondents highlighted five major areas of concern:

- Targets are more difficult to achieve (32% of responses)
- Bonuses were not paid this year, leading to personal financial pressures (29%)
- A belief that competitors are paying bribes to win contracts

and, thus, an incentive to follow suit (26%)

- A desire to make the numbers in order to earn performance bonuses (24%)
- At corporate level, senior management want to report a desired level of financial performance (18%)

## Types of economic crimes

Economic crime takes on many different forms, some more common than others, but all can be equally damaging if they occur.

Asset misappropriation has always been the most common form of economic crime. The prevalence of this type of fraud is not surprising, as it is among the easiest to commit and to detect.

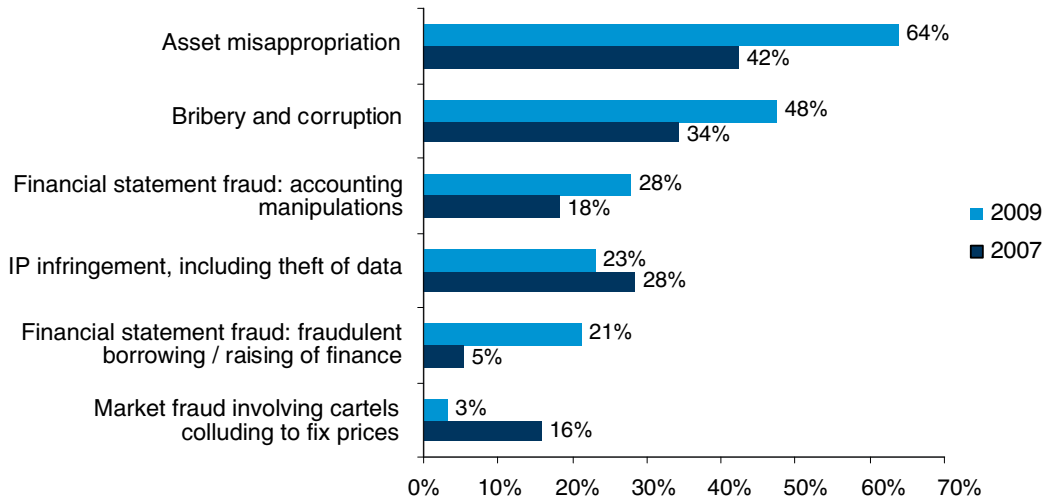
Covering a wide range of crime from theft of cash or inventory to fraudulent

disbursements, our survey provides a clear indication of where management should concentrate its immediate attention in order to avoid losses.

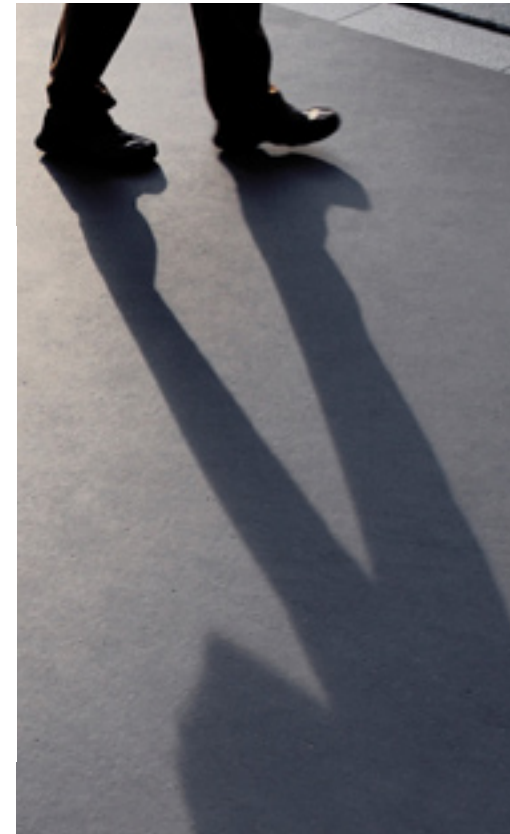
Bribery and corruption remains a major issue for Russian companies. Of the companies surveyed, 48% suffered from an instance of bribery or corruption in the last 12 months. This is twice the global average, emphasising the challenge faced by government and business in tackling the cancer of corruption in Russia.

In 2009, we see that financial statement fraud has become increasingly prevalent. The significant increase in this type of fraud may result from failures in controls arising from budget cuts in response to the economic climate, combined with pressure to meet increasingly difficult financial targets.

Figure 3. Actual incidence of fraud\*



\*% of respondents who experienced economic crimes in the past 12 months



## Given this globalisation of anti-corruption, organisations should consider:

- Performing due diligence on their business partners, personnel and contracts involved in a new-market expansion
- Streamlining and integrating payment systems to easily see where, why and how much money is being spent
- Regularly testing payment systems and controls to ensure all expenditures are accounted for – at all times
- Issuing clear organisation policy on what constitutes unacceptable behaviour, and enforcing the prescribed consequences
- Thoroughly (and annually) training employees to address the impacts of international anti-corruption standards
- Performing frequent field tests to determine whether employees understand organisation compliance policy

## The financial and non-financial damage from economic crimes

### Direct cost

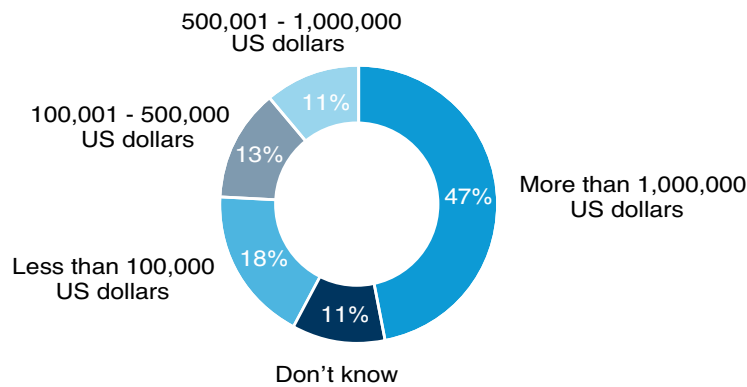
Fraud losses continue to run at high levels. Some commentators estimate

losses from fraud as high as 7% of revenue<sup>7</sup>. In our 2009 survey, 43% of Russian companies reported an increase in the cost of fraud as compared to 12 months ago. For 47% of companies, losses topped USD 1 million (see fig. 4). Despite a 17% decrease in comparison

with 2007 survey results, this number is still significant compared to CEE (24%) and global (17%) responses. Consistent with our previous surveys, larger companies have reported more frauds (see fig. 5), and high-value financial losses were most notably reported

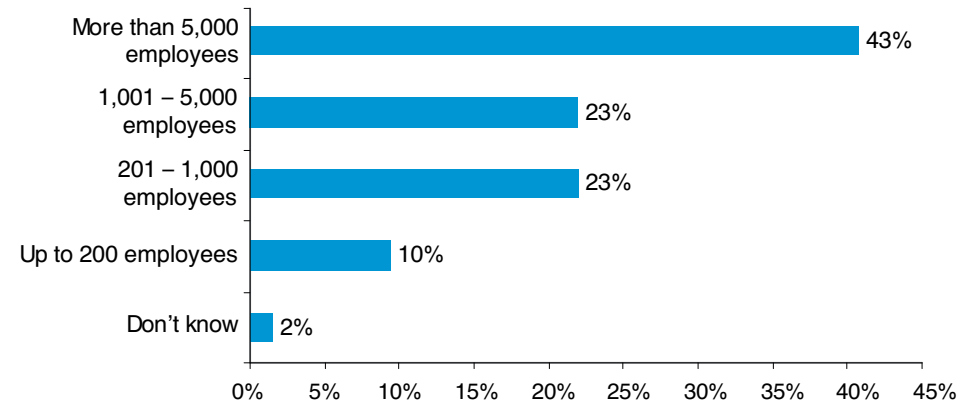
by financial services and energy, utilities & mining groups. The nature of these industries means that they are particularly exposed to both asset misappropriation and corruption, the two most prevalent types of economic crime.

Figure 4. Financial losses from economic crimes in the last 12 months\*



\*% of respondents who experienced economic crimes in the past 12 months

Figure 5. Companies reporting fraud, according to their number of employees\*



\*% of respondents who experienced economic crimes in the past 12 months

<sup>3</sup> Association of Certified Fraud Examiners 2008 Report to the Nation on Occupational Fraud and Abuse

## Collateral damage

While the direct costs of economic crime may seem alarming enough on their own, one should not ignore the collateral damage from fraud, i.e., damage to a company's brand and customer trust; to the market and shareholder trust; to the company's business relations and relations with regulators; and to staff morale, which can result in high staff turnover and loss of productivity. Although difficult to quantify, the collateral damage

from fraud can be a significant cost to any business.

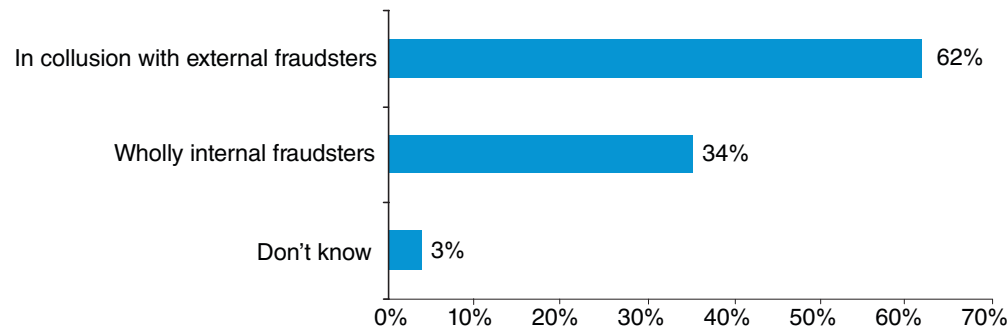
Some 44% of Russian companies highlighted employee morale as the most significant factor affected by economic crime. The importance of staff morale to the success, reputation, productivity and efficiency of any organisation as well as the additional costs incurred due to the resultant high staff turnover should be incentive enough for executive management to act decisively on fraud prevention measures.

Compared to other territories, external parties appear to play a more significant role in Russia in carrying out economic crimes. 62% of Russian companies believe that a party external to the company played a role in the fraud (see fig. 6). This may well be due to Russian

business's increased reliance on intermediaries, agents, joint venture partners and other middlemen. Unless properly controlled, these external relationships can easily get out of hand and expose the company to heightened economic crime risk.

## Perpetrators of fraud

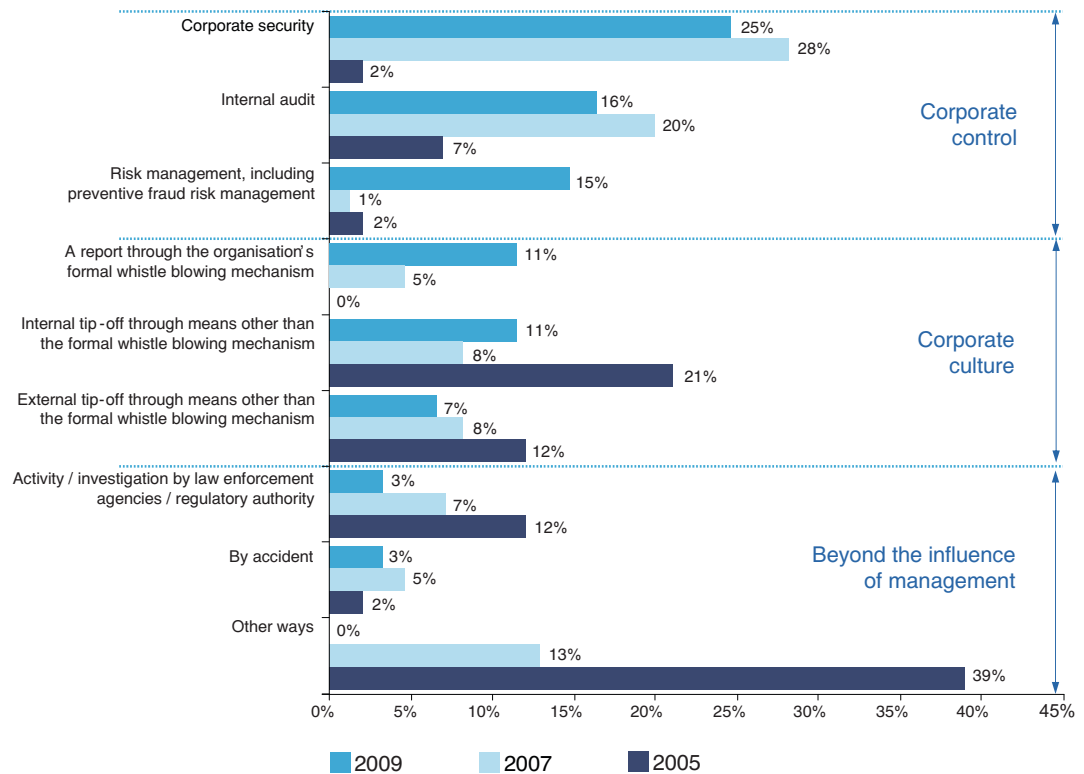
Figure 6. Perpetrators of fraud\*



\*% of respondents who experienced economic crimes in the past 12 months

## Fraud – look, and you will find

Figure 7. Detection methods\*



\*% of respondents who experienced economic crimes in the past 12 months

The trends noted in the previous Economic crime surveys continues – Russian organisations are more proactively addressing fraud risks and strengthening their risk management systems. In the last 12 months:

- 63% of the Russian respondents implemented additional procedures to check the identity of customers and suppliers
- 52% – cited increased attention by internal audit
- 49% – improved tone at the top to reinforce ethical behaviour
- 47% – implemented additional recruitment and exit procedures
- 38% – reviewed anti-fraud policies

A correlation was found between the frauds reported and the frequency of fraud risk assessments performed by companies. Where fraud risk assessments were conducted on a frequent basis, 42% of the respondents reported incidences of economic crime. It appears that those organisations who conduct frequent fraud risk assessments were able to detect more fraud and, as such, reported more frauds.



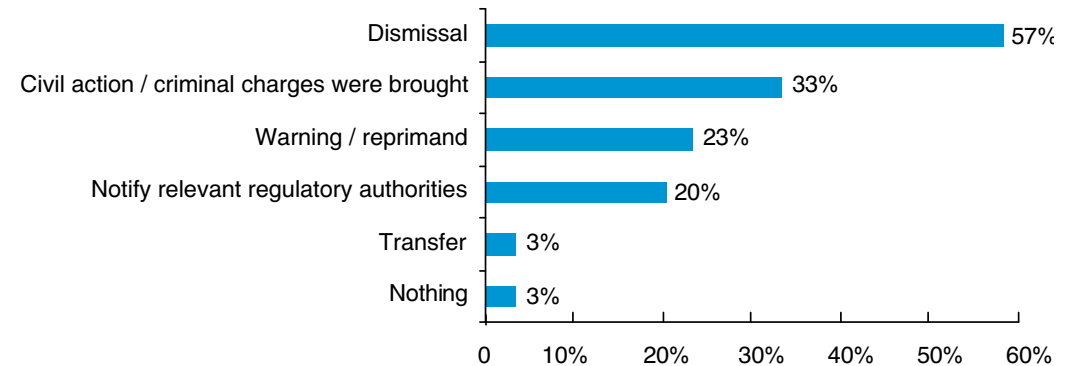
### Time for action – dealing with fraudsters

Once a company confirms a suspected fraud, appropriate action against the perpetrator is essential in order to deter other potential fraudsters and to show stakeholders in the business that the organisation will not tolerate such malpractice. Dismissal remains the favoured route for dealing with internal offenders. It is worth noting that this

rate is significantly lower in previous surveys: 25% in 2007 and 15% in 2005.

And while the number of respondents claiming they commence legal action may seem high, it is perhaps most pleasing to note that the percentage of companies doing nothing against internal and external perpetrators decreased by 11 percentage points compared to 2007 – clearly a move in the right direction.

Figure 8. Actions taken by companies against internal perpetrators\*



\*% of respondents who experienced economic crimes in the past 12 months

## Fraud in the future

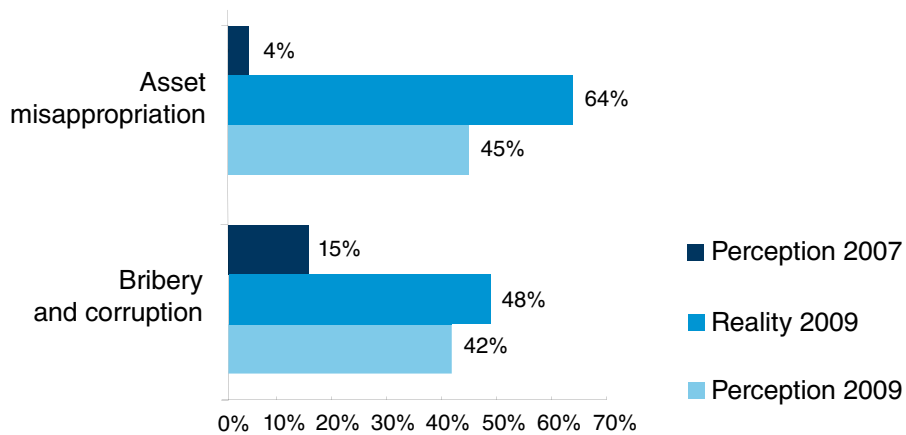
Economic crime is and will remain a very serious risk for Russian organisations.

The economic downturn is changing the nature and scale of the fraud and integrity risks that organisations face. The speed of change is such that opportunities to commit fraud will be prevalent. More people will feel real pressure to ‘cross the line’ or to look the other way while others do so. In addition, the falling economic tide will

expose more frauds that were ongoing while economic conditions were good. Asset misappropriation and bribery and corruption are the two forms of crime that respondents believe their organisations will most likely experience in the next 12 months.

Although there has been an increase in the perception levels, the results show a significant gap between the perception of the likelihood that fraud will occur in future compared with the reality of incidence of fraud historically reported.

**Figure 9.** Perception that fraud will occur in future in 2007 and 2009 and reality of incidence of fraud in 2009\*



\*% of all respondents

## Recommendations: the strategy of the enlightened organisation

In our more detailed study *Fraud in a Downturn*<sup>4</sup>, we looked in depth at 11 key issues facing organisations today and provided a roadmap for the enlightened organisation.

One hears commentators on fraud describing how a particular solution is key

to the management of fraud risk – ‘risk identification’, ‘the tone at the top’ or ‘better use of technology’ are just a few of the many keys that seem to be available.

In our experience, the enlightened organisation evaluates the options available to reduce fraud losses within a comprehensive framework of the kind we show below.

**Figure 10.** The PricewaterhouseCoopers Fraud Wheel<sup>5</sup>



<sup>4</sup> [www.pwc.ru/forensic/eng](http://www.pwc.ru/forensic/eng)

<sup>5</sup> In 1992, the Committee of Sponsoring Organizations of the Treadway Commission (COSO) developed a model for evaluating internal controls. This model has been adopted as the generally accepted framework for internal control and is widely recognised as the definitive standard against which organisations measure the effectiveness of their systems of internal control. We have adapted the COSO framework to illustrate some of the key elements of a fraud and integrity risk control framework.

Each organisation must determine how best to implement a fraud and integrity risk strategy. We set out below some of the questions those charged with governance need to ask, and receive answers to, in order to obtain some comfort that a sound strategy is in place:

- **Organisational tone** – What steps are being taken to be certain that the right tone at the top permeates down through the organisation? Does our remuneration strategy, including bonus arrangements, support the organisation's ethical stance, or undermine it?
- **Governance** – Are we receiving sufficient information and asking enough questions to have a sound strategic oversight of fraud risks, losses and prevention programmes? What are we doing personally to promote an anti-fraud culture?
- **Fraud and integrity policies** – Do we have the right policies and practices in place (code of conduct, fraud policy, whistle blowing, conflicts of interest, fraud response) and, more importantly, are they adequately publicised, promoted and enforced?

- **Hiring and promotion** – How much do we know about the people we recruit or promote to positions of responsibility? Is there anything else we should know before we bring them in or promote them?
- **Risk assessment** – What are the key fraud and integrity risks? Who is making this assessment and what information is the assessment based on? Has anyone thought through the fraud and integrity risks arising from the people we do business with, i.e., our sales agents, distributors, joint venture partners and suppliers?
- **Control linkage and evaluation** – Is the control system designed principally to identify errors, or is it sufficiently robust to prevent or detect fraud, corruption or other misconduct risks? Are we using best practice unpredictable controls, including spot checks and data mining, to help both detect and deter potential fraudsters? Do we have a reliable, trusted whistle blowing programme (an essential anti-fraud and corruption control)?
- **Management information** – Do our middle and senior management have

the information they need to manage fraud and integrity risks? A sound information system will include reliable fraud loss reporting as well as data on ongoing internal investigations and whistle blowing activity.

- **Communication and training** – Do our people receive proper communication and training? Are operational and finance staff an effective first line of defence against fraud and integrity risks? Have staff been trained to identify fraud and integrity risks in their business areas and to develop preventative and detective controls that really work?
- **Management oversight** – Do senior management monitor fraud, corruption and other integrity-based threats and take action where needed? Senior management should monitor compliance with key policies and the delivery of training programmes around business ethics.
- **Gatekeeper functions** – Are teams working together in the right way to reduce fraud, corruption and other integrity risks? Are gatekeeper functions such as loss prevention teams, in-house legal, security, internal

audit and the compliance function working together to deliver an effective fraud and integrity risk strategy?

- **Fraud and corruption response** – How well do we deal with allegations of fraud and corruption when they arise? Are we conducting thorough, independent reviews and taking action where appropriate? How do we ensure that lessons learned from the reviews are implemented across the company, and not only in the area affected by the fraud?

It is for those charged with governance to take the lead on fraud and integrity issues. Employees look to the board and senior management to set the tone, and unless the senior commitment is there, change will not happen and the benefits of reducing fraud and other integrity risks will not be realised.

The good news is that effective fraud risk management more than pays for itself. Companies across industry sectors are desperate to find ways to reduce cost. Attacking fraud, waste and abuse offers a huge cost savings opportunity for a relatively low investment.

PricewaterhouseCoopers ([www.pwc.ru](http://www.pwc.ru)) provides industry-focused assurance, tax and advisory services to build public trust and enhance value for our clients and their stakeholders. More than 163,000 people in 151 countries across our network share their thinking, experience and solutions to develop fresh perspectives and practical advice.

### Forensic services

With the largest network of forensic services practices in the world, spanning 63 countries and employing over 1,400 advisors, PricewaterhouseCoopers firms can draw on vast experience of dealing with difficult situations across a broad spectrum of industries in many jurisdictions. Our fast-growing Forensic services practice in CEE employs over 70 professionals, including accountants, economists and IT professionals.



## Contact information



**John Wilkinson**

Partner  
Forensic services leader  
CEE, Russia and CIS



**Inna Fokina**

Director  
Accounting investigations,  
commercial disputes,  
transaction and shareholder  
disputes



**Irina Novikova**

Director  
Accounting investigations,  
fraud risks and controls

Tel: + 7 (495) 223-5046

Fax: + 7 (495) 967-6001

