

Shifting beyond our borders: Economic Crime in Singapore



24%

1 in 4 Singapore-based respondents have experienced some form of economic crime in the last two years.

80%

Asset misappropriation remains the most commonly experienced economic crime in Singapore and globally.

70%

Most Singapore-based respondents have operations in countries with high levels of corruption risk.

Contents

| | | |
|-----------|--------------------------------|----|
| 3 | Foreword | |
| 4 | The Big Picture | |
| | <i>Types of Economic Crime</i> | 5 |
| | <i>Asset missappropriation</i> | 6 |
| | <i>Bribery and corruption</i> | 6 |
| | <i>Cybercrime</i> | 8 |
| | <i>Procurement fraud</i> | 10 |
| 11 | Detecting fraud | |
| 14 | Terminology | |



Although Singapore-based companies are reporting lower incidences of fraud relative to the global average, we cannot be complacent as the battle against white collar crime is an ongoing one, and an increasingly borderless one.

Foreword

It will surprise few to learn that the incidence of economic crime reported in Singapore – such as procurement fraud, cybercrime, bribery and corruption - is lower than the rate recorded globally. Singapore’s reputation as a safe and transparent place to do business is reflected in the views of the Singapore-based respondents to our 2014 Global Economic Crime Survey¹.

While this is encouraging, the risk of fraud for companies operating in Singapore as well as globally continue to evolve. Increasing reliance on technology poses great threats in the form of cybercrime, as evidenced in the several high profile incidents which have occurred in Singapore in the last few months. In addition, ongoing globalisation means that many Singapore-based companies are now doing business in environments with inherently higher corruption risks.

Although the Singapore respondents are generally reporting lower incidences of fraud relative to the global average, we cannot be complacent as the battle against white collar crime is an ongoing one, and an increasingly borderless one. Businesses need to continually assess the mechanisms they have in place for dealing with these risks, and consider if their current strategies are adequate in view of the increasing threats.

The Singapore edition of our 2014 Global Economic Crime survey turns the spotlight to the types of economic crime most commonly experienced in Singapore, together with the biggest perceived impacts on organisations. The report also provides guidance on how companies can manage these risks.

We trust that the report will be a valuable resource to stakeholders in all areas of your business. As the old Chinese Sun Tze saying goes, “know thy self and enemy to be successful” (知己知彼, 百战不殆) - companies that understand their risk environment well and mitigate these threats appropriately will be poised to limit their losses to economic crime and be better positioned to respond to the ever changing global business environment we operate in.

Chan Kheng Tek
PwC Singapore Forensics Leader
February 2014

¹ Throughout this report we refer to “Singapore-based” organisations, which consist of both local Singaporean companies or multinationals based in Singapore.

In the last 24 months, one in four (24%) Singapore-based companies have experienced economic crime relative to one in three companies globally (37%).

The Big Picture

Our survey revealed that in the last 24 months, one out of every four Singapore-based companies (24%) experienced some form of economic crime. This result is certainly favourable relative to the global average of more than one third (37%). The number of incidents of economic crime experienced by Singapore companies was also significantly lower than the global average. Of the Singapore companies that suffered from some type of economic crime, 80% reported fewer than 10 incidents over the last 24 months as compared to the global average of 61%.

These results are not surprising given the strong emphasis on governance and controls in both the private and public sector in Singapore. The clean and transparent business environment coupled with our strong legal framework explains why Singapore ranks very highly in many global business surveys, such as the Transparency International's Corruption Perception Index 2013, in which Singapore received a fifth place ranking out of 177 countries and territories.² However, despite the good governance and safe business environment, one out of every four Singapore businesses still suffer fraud, and there is much high profile evidence of these cases occurring both in the private and public sector.

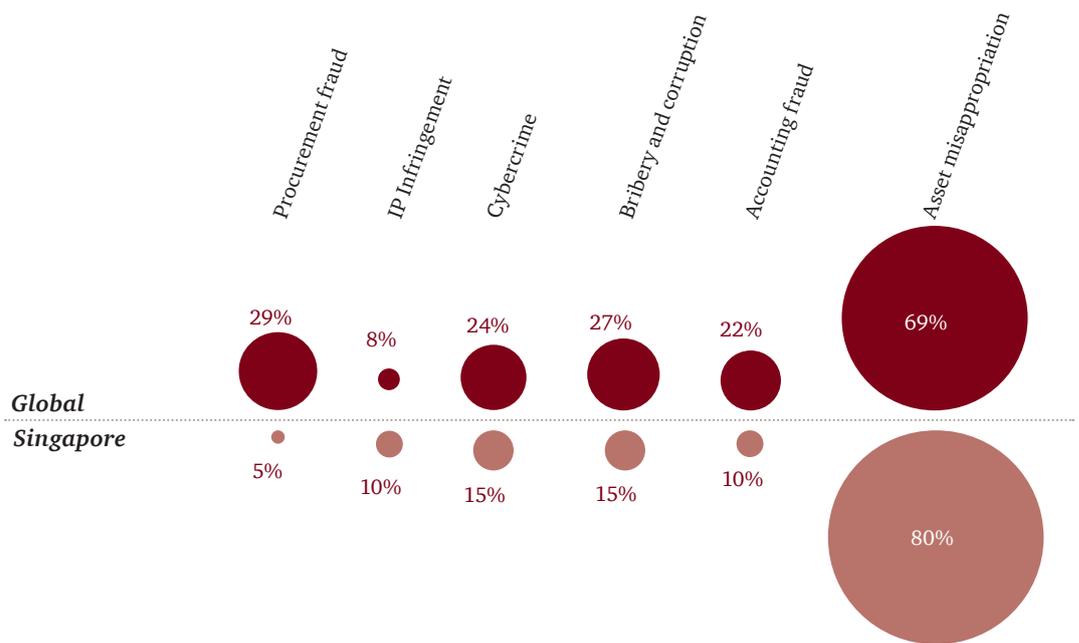
The message for Singapore-based companies is therefore clear - fraud is not something that can be eliminated. Organisations need to resist the temptation to become complacent. As our business environment and society evolve, and Singapore companies continue to expand beyond our borders, companies need to be vigilant and continually assess the risk of fraud.

² 2013 Corruption Perceptions Index, Transparency International, 2013

Types of Economic Crime

Our survey results show that the main economic crimes experienced by Singapore-based companies were asset misappropriation (80%), followed by bribery and corruption (15%) and cybercrime (15%). Globally, asset misappropriation (69%), procurement fraud (29%), bribery and corruption (27%) and cybercrime (24%) featured as the most frequently experienced types of economic crime.

What types of economic crime has your organisation experienced within the last 24 months?³



³Note respondents may have experienced one or more types of economic crime in the last 24 months.

Asset Misappropriation

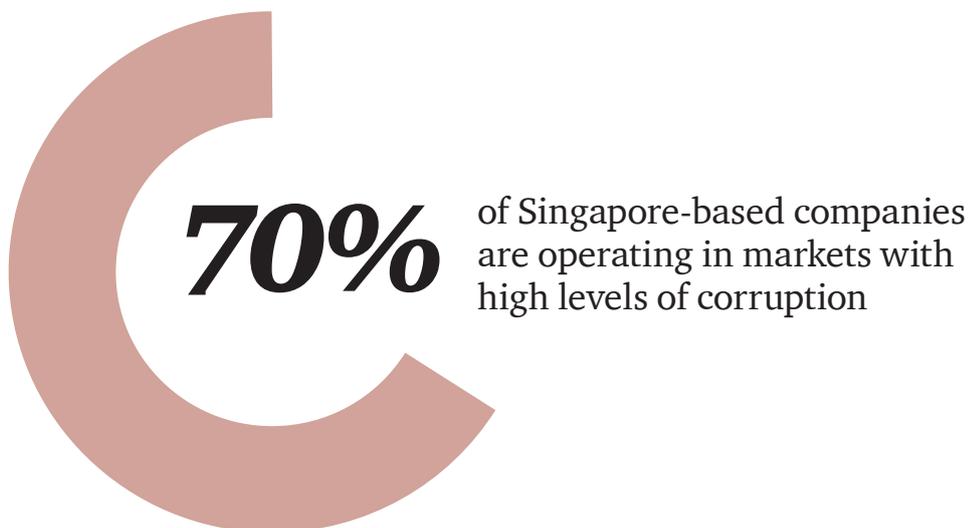
Asset misappropriation continues to be the most commonly experienced type of economic crime both in Singapore and globally.

The relatively high rate of asset misappropriation is consistent with what we regularly see in the whistle blowing investigations we have been involved in. In most circumstances, the key elements of the fraud triangle (pressure/motivation, opportunity and rationalisation) converge, causing staff members to turn to crime to finance their lifestyle (e.g., credit card or gambling debts or other financial pressure creates a motivation to commit fraud). Typically, the root cause for this type of fraud is due to a misplaced reliance on trust coupled with a weak compliance culture or attitude towards controls in the organisation (opportunity). The longer the perpetrator is employed by the company, the higher the level of reliance on trust in these long serving employees, which creates a false sense of security amongst management. Under such circumstances, the perpetrator may succumb to the temptation to dip their hands into the company's coffers and try to justify their actions based on some sense of entitlement (rationalisation).

Bribery and Corruption

Due to a strong and efficient local legal framework, strict deterrence in the form of punishments, as well as the typically strong culture of anti-bribery/ anti-corruption compliance, only 15% of Singapore respondents reported incidents of bribery and corruption as compared to 27% of global respondents.

However, it is important to note that the risk of corruption for Singapore-based companies extends beyond Singapore. Our survey also found that 70% of Singapore-based respondents have operations in markets with high levels of corruption risk (compared to 50% globally). Increasing globalisation and the need for Singapore companies to look beyond the domestic market to stay competitive has resulted in 60% of Singapore-based companies pursuing an opportunity in a market with a high level of corruption in the last two years (compared to 38% globally). More than half of the Singapore-based respondents perceive that corruption/bribery is the highest risk in doing business globally compared to other risks such as money laundering and competition law.





Bribery in Singapore and beyond

In 2013, Asian regulators stepped up enforcement efforts to crack down on bribery and corruption. There have been several examples of Singapore registered companies who have been allegedly involved in bribery or corruption outside of Singapore. Some recent cases include:

- i. Bribery by a Singapore contractor - a Singapore-based contractor was charged in connection with alleged bribes paid to a US Navy ship commander and a Naval Criminal Investigative Service agent in exchange for information relating to the worldwide movement of Navy ships. The charges resulted in the loss of hundreds of millions of dollars in US Navy contracts affecting not only the specific entity but other Singapore businesses involved in the supply chain as well.⁴
- ii. Bribery of an Indonesian oil and gas official - a Singapore-based crude oil trader is alleged to have made significant cash bribes and offered gifts to an executive with Indonesia's oil and gas regulator in order to gain favour in crude oil tenders.⁵

This trend reflects the greater importance for Singapore companies to perform risk-based due diligence on international business partners to mitigate potential bribery and corruption risks. Taking such preventive actions and implementing a robust anti-bribery and corruption compliance programme will substantially lessen the risk of falling prey to these types of crimes. In addition, doing so may also help companies avoid the wrath of the regulators in the event of a bribery investigation. In one recent case involving a Singapore-based employee of a major financial institution, US regulators dropped all charges against the organisation but prosecuted (and jailed) the rogue employee. The charges against the organisation were dropped on the basis that its compliance programme was sufficiently robust to provide “reasonable assurance” that its employees were not bribing government officials.

⁴ <http://www.reuters.com/assets/print?aid=USBRE99L00620131022>

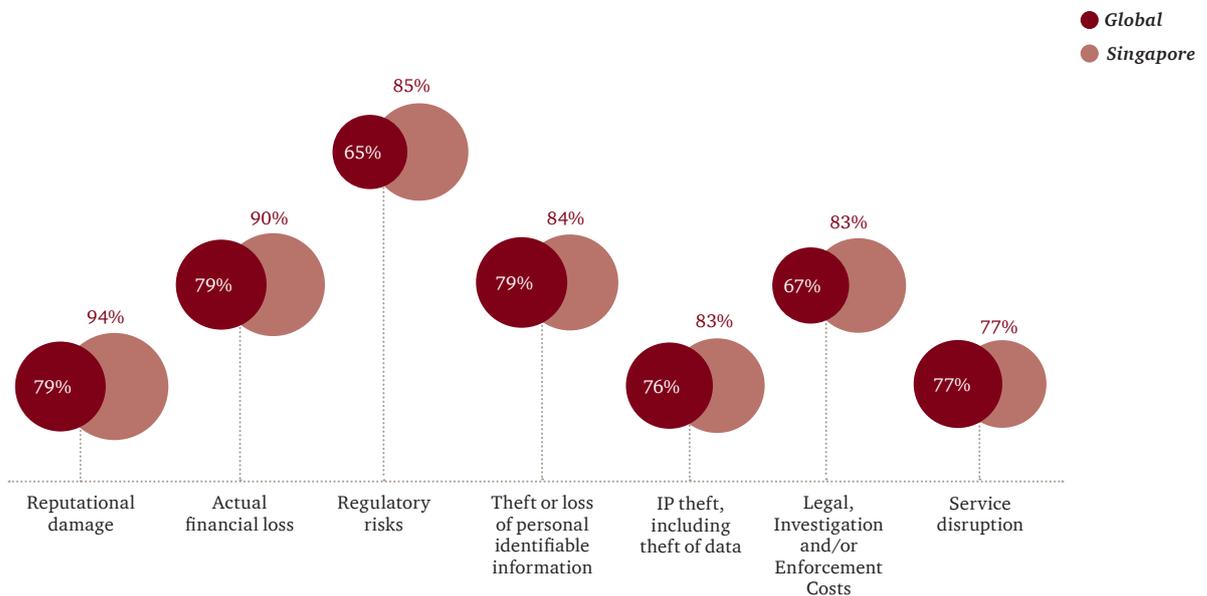
⁵ <http://sg.finance.yahoo.com/news/indonesia-energy-regulator-chief-detained-114731010.html>

Cybercrime

Singapore respondents reported fewer cyber incidents compared to global respondents, at 15% and 24%, respectively. While the survey revealed fewer cybercrime episodes in Singapore, the risk of cybercrime occurring here is clear and present. In our recent annual Global CEO Survey, PwC asked over 1,300 CEOs what they thought would be the next big thing to revolutionise their business, industry or society over the next 10 years. Somewhat unsurprisingly, technology was the most common response.⁶ The various technologies underpinning this revolution are creating exciting opportunities for companies but also include a range of risks. These risks are evident from several prominent and high impact cyber incidents which have taken place in Singapore in the last 12 months, including:

- i. In June 2013, a Singaporean traditional chinese medicine company had its website hacked and defaced with messages.⁷
- ii. In November 2013, a Singapore government website was hacked into. The website's search function was impaired and images were overlaid on the webpage.⁸
- iii. In December 2013, the Singapore branch of an international bank discovered that close to 650 of its private bank clients' details had allegedly been stolen. The purported theft of the bank statements did not occur through the banks' IT and data system. Instead the information was allegedly stolen from one of the servers of a third-party service provider which was hired by the bank to print bank statements.⁹

How concerned are you about the effects of each of the following types of cybercrime activity on your organisation?



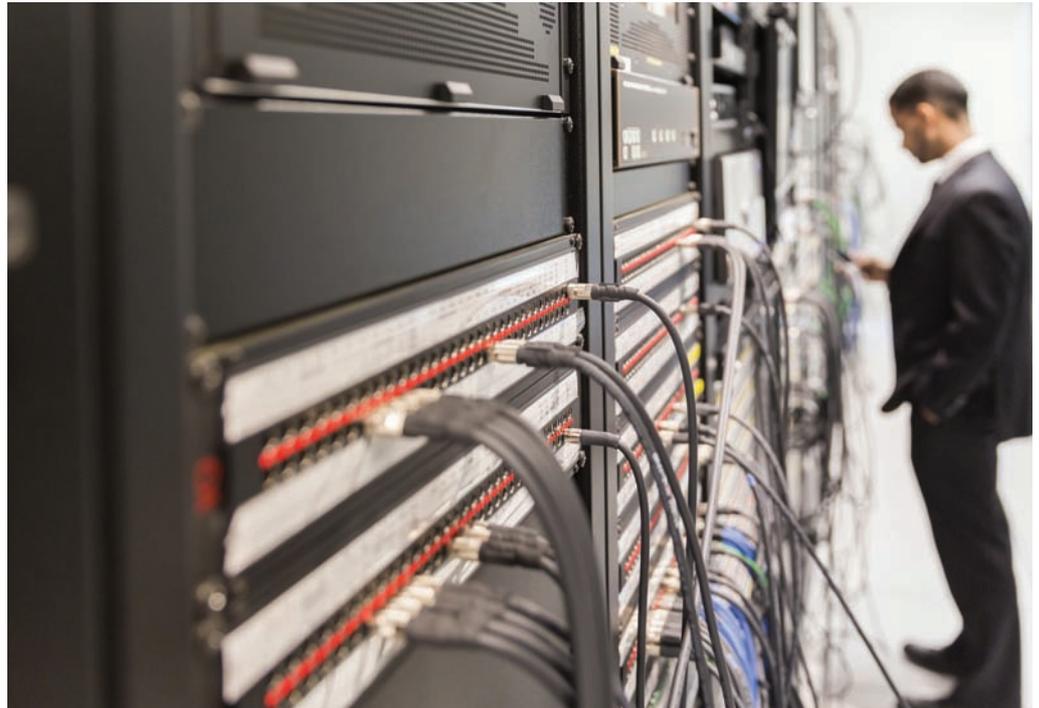
⁶ "Fit for the future: Capitalising on global trends" 17th Annual Global CEO Survey, PwC, 2014

⁷ www.straitstimes.com/breaking-news/singapore/story/hackers-deface-eu-yan-sang-website-leave-haze-related-messages-2013062

⁸ <http://www.straitstimes.com/breaking-news/singapore/story/subpage-the-prime-ministers-office-website-hacked-investigations-ongoing>

⁹ <http://www.straitstimes.com/breaking-news/money/story/account-information-stolen-nearly-650-clients-stanchart-singapores-private>

Organisations must ensure their cyber security policies and controls are implemented appropriately and continually test the effectiveness of these efforts.



Despite the low incidence of cybercrime recorded in our survey, Singapore respondents are still rightly concerned over the various negative effects of potential cybercrime activity, with reputation damage listed as their biggest worry, followed by actual financial losses and regulatory risk. In response to the ongoing threats posed by cybercrime, on 15 January 2014, the Infocomm Development Authority (IDA) announced that the global network security firm FireEye had teamed up with IDA to open a facility dedicated to developing expertise in cyber security.¹⁰

The above measures are strengthened by Singapore's well-established legal and regulatory environment with regards to cybercrime (e.g., the Computer Misuse and Cybersecurity Act, MAS Internet Banking and Technology Risk Management Guidelines, and Instruction Manual 8 for the Singapore Government). Most recently, Singapore also enacted the Personal Data Protection Act (PDPA) which governs the collection, use, disclosure and care of personal data. The main data protection rules will come into force in July 2014. Organisations have the opportunity to strengthen their cyber security policies and controls by implementing a programme in compliance with the PDPA.

While the regulatory framework provides mandates and guidance, organisations must ensure their cyber security policies and controls are implemented appropriately, and continually test the effectiveness of these efforts. As companies increasingly rely on IT and electronic data, the use of automation in cyber security, policy compliance and data analytics becomes more important. Lastly, businesses also need to consider implementing and testing their cyber incident management capabilities, so that they will be able to effectively react to an incident when it occurs.

¹⁰ <https://www.ida.gov.sg/About-Us/Newsroom/Speeches/2014/Speech-by-Ms-Jacqueline-Poh-of-IDA-at-the-Opening-of-Fireeyes-Centre-of-Excellence>

As Singapore companies continue to expand their footprint in the region, procurement functions will be exposed to environments where fraud is a greater risk.

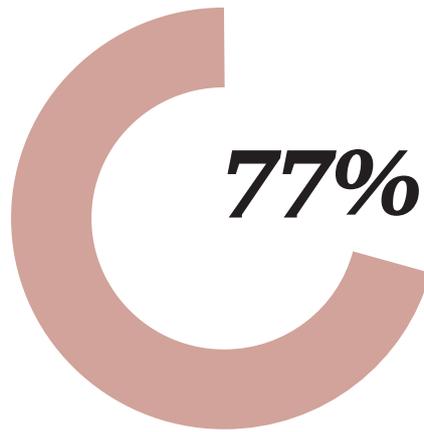


Procurement Fraud

In Singapore, companies experienced a significantly lower rate of procurement fraud as compared to the global survey respondents (5% compared to 29%). All of the Singapore-based respondents who reported procurement fraud in the last 24 months experienced it in the vendor selection process. There was not a single reported incident of fraud in the bid process, contracting or the payment process.

However, companies should again resist the temptation to become complacent in relation to procurement. Examples of common procurement fraud we continue to see in our investigations include incidences of theft of inventory, manipulation of bids by multiple vendors, kickbacks to procurement officers through inflated price of purchases and payment of bribes to buyers to place suppliers on the approved vendor list.

As Singapore companies expand their footprint in the region, the procurement department will be exposed to environments where fraud is a greater risk, and the individuals exposed to these challenges have to be well prepared to mitigate these potential procurement risks.

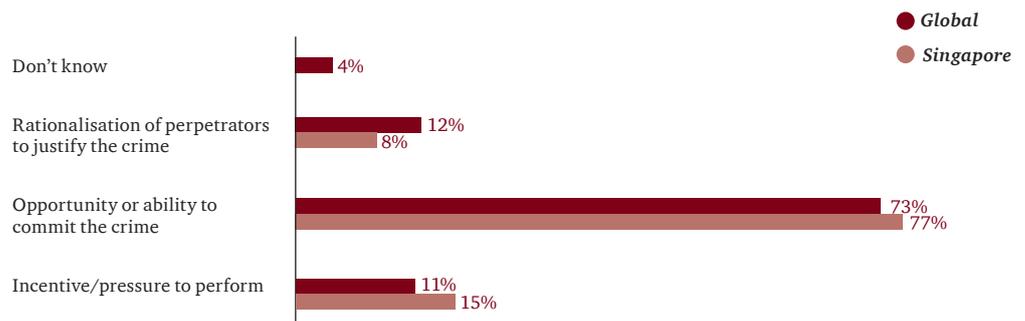


of Singapore companies felt the biggest factor contributing to economic crime occurring is opportunity or ability to commit the crime.

Detecting Fraud

A significant majority of Singapore companies (77%) stated that the biggest factor contributing to economic crime occurring was opportunity or the ability to commit the crime. This reinforces the importance of a strong internal control framework coupled with a rigorous approach to compliance to minimise opportunities to commit economic crime.

What factor do you feel has contributed the most to economic crime committed by internal actors?

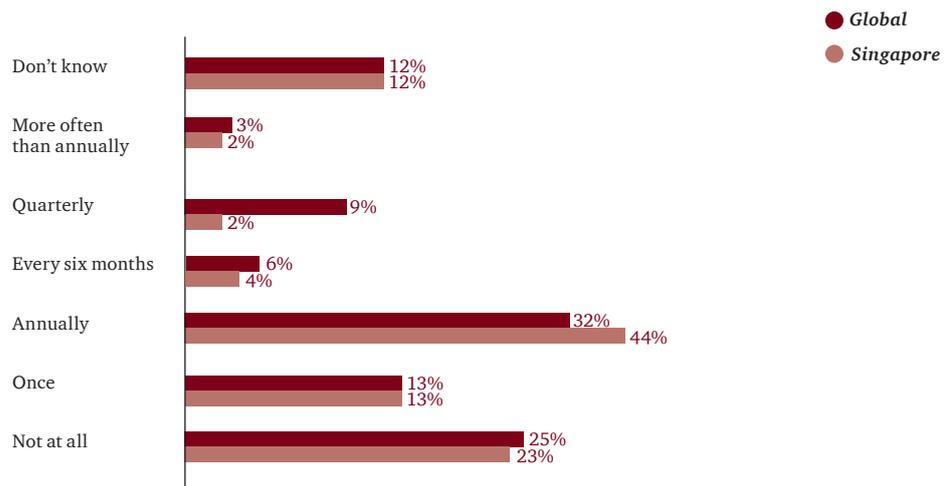


Encouragingly, our survey showed that the majority of Singapore companies do conduct fraud risk assessments. The percentage of companies which conducted a fraud risk assessment in the past two years does not vary significantly between Singapore (65%) and the global average (63%). Singapore companies tend to rely on annual assessments (44% compared to 32% globally), whereas global respondents seem to perform these more frequently, with 15% conducting assessments on a quarterly or half yearly basis, compared to 6% of Singapore-based respondents.

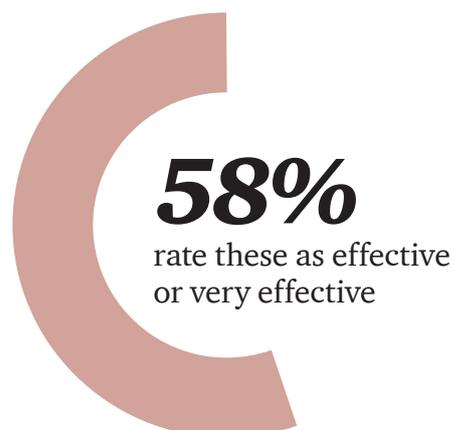
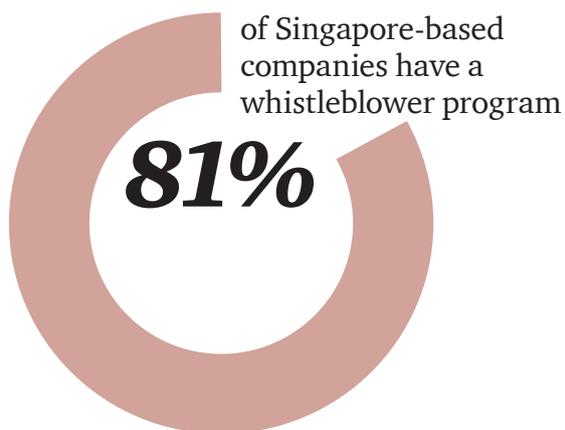
A fraud risk assessment is a tool that enables businesses to better mitigate risks through the introduction or strengthening of controls. The benefits of a fraud risk assessment include the identification of departments that pose the greatest risk of fraud; the evaluation of existing controls to determine whether they are operating effectively; and the identification of gaps where additional controls are needed.

Notwithstanding the above, there remains a significant percentage of companies both in Singapore and globally (35% and 37%, respectively) that do not conduct fraud risk assessments or are unaware if they do. The reasons given by Singapore respondents for not conducting a fraud risk assessment was a perceived lack of value (37%) and being unsure what a fraud risk assessment entails (21%).

In the last 24 months, how often has your organisation performed a fraud risk assessment?



Apart from fraud risk assessments, whistleblower programmes have been gaining traction and are now widely adopted in Singapore. Singapore companies with whistleblower programmes have increased more than two-fold from a 35% adoption rate in 2005¹¹ to 81% in 2013. Not only is the adoption rate higher than the global rate of 62% in 2013; of the 81% of Singapore companies that have a whistleblower programme, 58% of these companies rate the whistleblower programme as effective or very effective as compared to 50% globally.

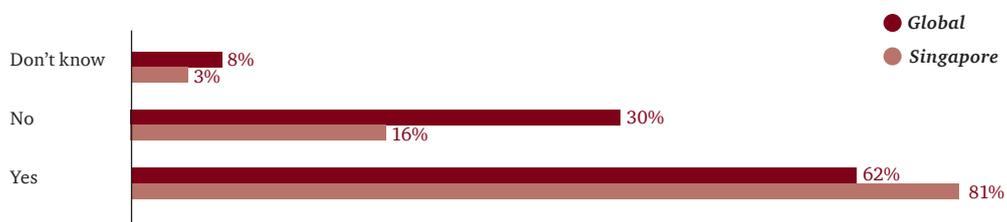


¹¹ Economic crime: people, culture & controls: The 4th biennial Global Economic Crime Survey, Singapore, PricewaterhouseCoopers

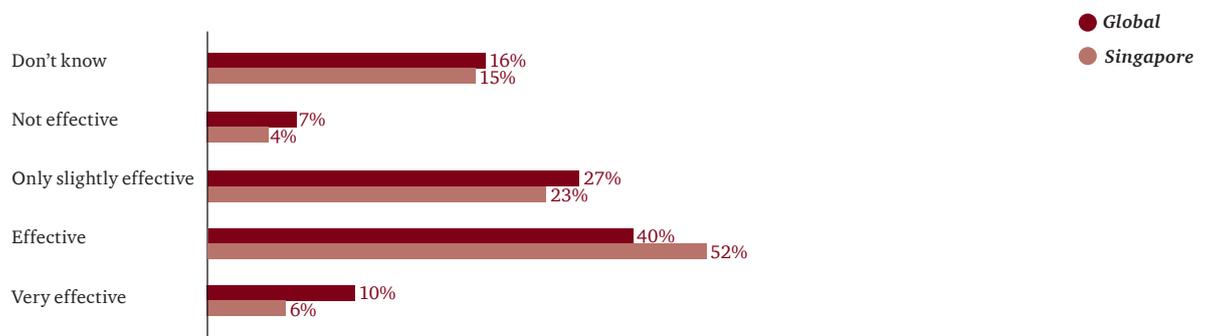


Fraud risk assessments are enabling many companies to better mitigate risks through the introduction or strengthening of controls.

Does your organisation in Singapore and Globally have a whistleblower mechanism?



How effective would you rate your whistleblowing mechanism in the prevention and detection of economic crime?



Terminology

Accounting fraud

Financial statements and/or other documents are altered or presented in such a way that they do not reflect the true value or financial activities of the 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 (including monetary assets/cash or supplies and equipment) by directors, others in fiduciary positions or an employee for their own benefit.

Bribery and corruption

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, 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.

Competition law/Antitrust law

Law that promotes or maintains market competition by regulating anticompetitive and unfair business practices conduct by organisations. Examples may include price fixing, excessive, predatory or discriminatory pricing, unfair trading terms, and tying (i.e., stipulating that a buyer wishing to purchase one product must also purchase all or some of his requirements for a second product).

Cybercrime

Also known as computer crime; an economic offence committed using the computer and internet. Typical instances of cybercrime are the distribution of viruses, illegal downloads of media, phishing and pharming and theft of personal information such as bank account details. This excludes routine fraud whereby a computer has been used as a by-product in order to create the fraud and only includes such economic crimes where computer, internet or use of electronic media and devices is the main element and not an incidental one.

Economic crime

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

Financial loss/Financial terms

When estimating financial losses due to fraud, the participants should include both direct and indirect loss. The direct losses are the actual amount of fraud and the 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 business opportunity”.

Fraud risk assessment

Fraud risk assessments are used to ascertain whether an organisation has undertaken an exercise to specifically consider:

- i. The fraud risks to which operations are exposed;
- ii. An assessment of the most threatening risks (i.e., Evaluate risks for significance and likelihood of occurrence);
- iii. Identification and evaluation of the controls (if any) that are in place to mitigate the key risks;
- iv. Assessment of the general antifraud programmes and controls in an organisation; and
- v. Actions to remedy any gaps in the controls.

Human Resources fraud (recruitment and/or payroll fraud)

Fraud committed by members of the Human Resources department, including payroll fraud, ghost employees, pay-to-work, recruitment (i.e., hiring friends and/or relatives, hiring unqualified individuals, falsification of documents, etc.).

Incentive/Pressure to perform

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

Insider trading

Insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. Insider trading violations may also include ‘tipping’ such information, securities trading by the person ‘tipped’, and securities trading by those who misappropriate such information.

IP infringement (including trademarks, patents, counterfeit products and services)

This includes the illegal copying and/or distribution of fake goods in breach of patent or copyright, and the creation of false currency notes and coins with the intention of passing them off as genuine.

Markets with a high level of corruption risk

While corruption risk levels can be subjective, for the purposes of this survey we suggest a territory with a 2013 Transparency International Corruption Perception Index (“CPI”) score of 50 or less be considered a market with a high level of corruption risk.

Money laundering

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

Mortgage fraud

Mortgage fraud schemes employ some type of material misstatement, misrepresentation, or omission relating to a real estate transaction which is relied on by one or more parties to the transaction.

Opportunity or ability

The individual finds some way that he/she can use (abuse) his/her position of trust to solve the financial problem with a low perceived risk of getting caught.

Procurement fraud

Illegal conduct by which the offender gains an advantage, avoids an obligation or causes damage to his 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

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

Singapore-based respondents

Companies who participated in the survey who are local Singaporean entities or multinational companies based in Singapore.

Contacts



Chan Kheng Tek
PwC Singapore Forensics Leader
+65 6236 3628
kheng.tek.chan@sg.pwc.com



Sam Kok Weng
PwC South East Asia Regional Forensics Leader
+65 6236 3268
kok.weng.sam@sg.pwc.com



Jimmy Sng
PwC Singapore
Technology Consulting Leader
+65 6236 3808
jimmy.sng@sg.pwc.com



Goh Thien Phong
PwC Singapore
Corporate Recovery Leader/Forensics Partner
+65 6236 4018
thien.phong.goh@sg.pwc.com

<http://www.pwc.com/sg/en/economic-crime-survey/index.jhtml>

PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 158 countries with close to 169,000 people who are committed to delivering quality in assurance, tax and advisory services. Tell us what matters to you and find out more by visiting us at www.pwc.com.

This publication has been prepared for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is given as to the accuracy or completeness of the information contained in this publication, and, to the extent permitted by law, PricewaterhouseCoopers does not accept or assume any liability, responsibility or duty of care for any consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.

© 2014 PwC. All rights reserved. Not for further distribution without the permission of PwC. "PwC" refers to the network of member firms of PricewaterhouseCoopers International Limited (PwCIL), or, as the context requires, individual member firms of the PwC network. Each member firm is a separate legal entity and does not act as agent of PwCIL or any other member firm. PwCIL does not provide any services to clients. PwCIL is not responsible or liable for the acts or omissions of any of its member firms nor can it control the exercise of their professional judgment or bind them in any way. No member firm is responsible or liable for the acts or omissions of any other member firm nor can it control the exercise of another member firm's professional judgment or bind another member firm or PwCIL in any way.