
KPMG
cutting through complexity
SMU
SINGAPORE MANAGEMENT UNIVERSITY
SINGAPORE FRAUD SURVEY 2014

FOREWORD

This is the fourth Singapore fraud survey report issued by KPMG, and the first time it has been undertaken with the support of the Singapore Management University.

We would like to thank all respondents for their time and effort in responding to this survey and for helping to make this report possible.

Besides providing you with an insight to the trends, nature and extent of fraud affecting organisations in Singapore, we hope it helps you understand the associated threats and how organisations here are managing the risks involved.

This year's survey suggests that internal fraud is becoming more prevalent and is often the result of inadequate internal controls. It also notes that internal controls are often either poorly implemented, easily overridden or poorly communicated.

Other significant threats which have come to the fore this year include overseas bribery and corruption, as well as e-crime. This may have been due to publicity surrounding corruption investigations in China, and the Heartbleed vulnerability.

We hope this report proves useful to you for benchmarking your company's preparedness to manage fraud risk and welcome any questions you may have.

Bob Yap
Head, Advisory
KPMG in Singapore

Professor Pang Yang Hoong
Dean, School of Accountancy
Singapore Management University

CONTENTS

EXECUTIVE SUMMARY

The findings of the KPMG-SMU Singapore Fraud Survey Report 2014 suggest that companies in Singapore are becoming increasingly proactive about implementing fraud risk management measures. While good progress has been made, there are significant opportunities for improvement in the implementation of anti-fraud measures.

KEY FINDINGS

FRAUD AFFECTS MORE THAN ONE IN FOUR COMPANIES IN SINGAPORE

29%

of respondents indicated at least one fraud incident had occurred in their organisation over the past two years

vs 22% in 2011

INTERNAL FRAUD HAS RISEN SINCE 2011 AND REMAINS THE MOST SIGNIFICANT THREAT

58%

of the fraud incidents reported in 2014 were perpetrated by employees

vs 47% in 2011

17%

of the fraud incidents reported in 2014 involved board members and senior management

unchanged from 2011

WHILE RECOGNISING THE THREAT OF FRAUD, COMPANIES CAN DO MORE TO IMPLEMENT ANTI-FRAUD MEASURES

53%

of respondents said fraud occurred due to weak or overridden internal controls, despite most having fraud risk management measures in place

59%

felt that employees were well informed of fraud risks, despite 85% saying that fraud and ethics policies were communicated to all staff

58%

monitored fraud risk indicators to pre-empt fraudulent activity while many regularly reviewed effectiveness of control measures

41%

communicated their fraud and ethics policies externally despite major concerns over third party conduct

BRIBERY AND CORRUPTION ARE OF GREAT CONCERN TO SINGAPOREAN COMPANIES DOING BUSINESS OVERSEAS

66%

were highly concerned about bribery and corruption risks

51%

were very concerned about payments or gifts related to wining or retaining business

ORGANISATIONS ARE INCREASINGLY CONCERNED ABOUT E-CRIME, ESPECIALLY WHEN IT COMES TO EMPLOYEE BEHAVIOUR.

64%

cited misuse of sensitive information

59%

cited falsification of records

51%

cited the manipulation of electronic audit trails

56%

cited the risk of confidential information being leaked via employee email

The overarching message from this survey is clear: it is important to have controls in place, but more work is needed to create a robust defence against fraud. Too often, anti-fraud controls were easily overridden, weakly implemented, poorly communicated or not monitored diligently.

1 FRAUD IN SINGAPORE

A. OCCURRENCE OF FRAUD

The risk of fraud remains a pervasive and persistent threat.

29%

were affected

vs 22% in 2011

While it is unclear whether occurrences are rising, or companies are simply getting better at detecting incidents, fraud risks are widespread and deserve closer attention.

B. PERPETRATORS OF FRAUD

The proportion of fraud perpetrated by employees has jumped to

58%

vs 47% in 2011

There was no change in the percentage of fraud incidents carried out by management (17%) such as board members and senior management.

Overall, internal fraud constituted 75% of fraud in 2014, up from 64% in 2011. It is noteworthy that fraud committed by internal parties was identified as a top concern in the 2011 report.

Comment

Companies in Singapore need to improve the way they implement anti-fraud policies and adopt best practices such as periodic monitoring and assessment.

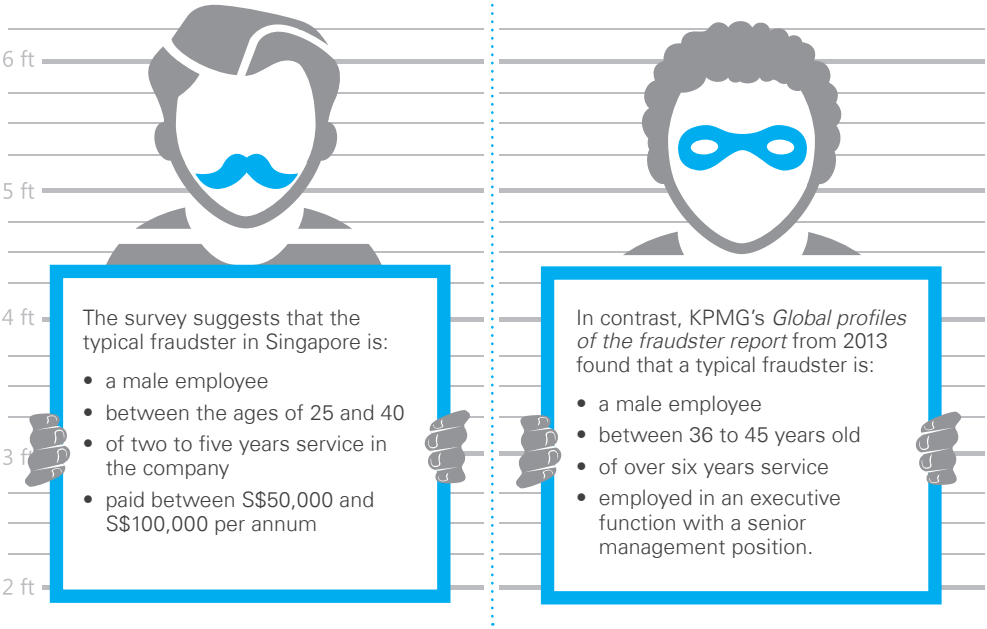
An organisation's board of directors plays a critical role in the oversight of programmes to mitigate the risk of fraud and misconduct.

Together with management, the board is responsible for setting the "tone at the top" and ensuring institutional support for ethical and responsible business practices in the organisation.

PERPETRATORS OF FRAUD

	2014	2011
Management	17 %	17 %
Employees	58 %	47 %
External Parties	25 %	36 %

SINGAPORE VS GLOBAL



The survey suggests that the typical fraudster in Singapore is:

- a male employee
- between the ages of 25 and 40
- of two to five years service in the company
- paid between S$50,000 and S$100,000 per annum

In contrast, KPMG's *Global profiles of the fraudster report* from 2013 found that a typical fraudster is:

- a male employee
- between 36 to 45 years old
- of over six years service
- employed in an executive function with a senior management position.

AGE OF FRAUDSTER

Under 25 years old

15%

25-40 years old

44%

41-55 years old

28%

Over 55 years old

13%

FRAUDSTER'S YEARS OF SERVICE

20%

34%

24%

22%

C. FRAUD DETECTION

The importance of a people-focused approach to fraud risk management is important as the survey suggests that more than half of fraud incidents were first detected by employees or customers.

Whistle-blowing channels were used by employees to report fraud in:

20%
of cases
vs 15% in 2011

What is unclear is whether occurrences are rising, or companies are simply getting better at detecting it.

17%
of fraud instances in 2014 were reported by employees through other channels

Customers play an important role too, as illustrated by the 17% of fraud incidents first detected as a result of notification by customers.

17%
were detected as a result of notification by customers

10%
were detected as a result of management review

As the power and prevalence of data analytics increase, it is likely that the use of technological solutions to identify fraud will continue to grow. One in 10 respondents said that fraud incidents were first detected by data analytics or other investigative procedures.

However, the role of external and internal audit in fraud detection declined.

- 3% of respondents said fraud incidents were first detected by external audit, down from 12% in 2011
- 3% of respondents said fraud incidents were first detected by internal audit, down from 15% in 2011.

COMMENT

Well-trained and security-conscious staff members can be a crucial first line of defence against fraud.

The quality of training is therefore important in raising employees' awareness of fraud risks and anti-fraud policies. Training therefore has to be tailored to make it relevant to different employee levels and functions.

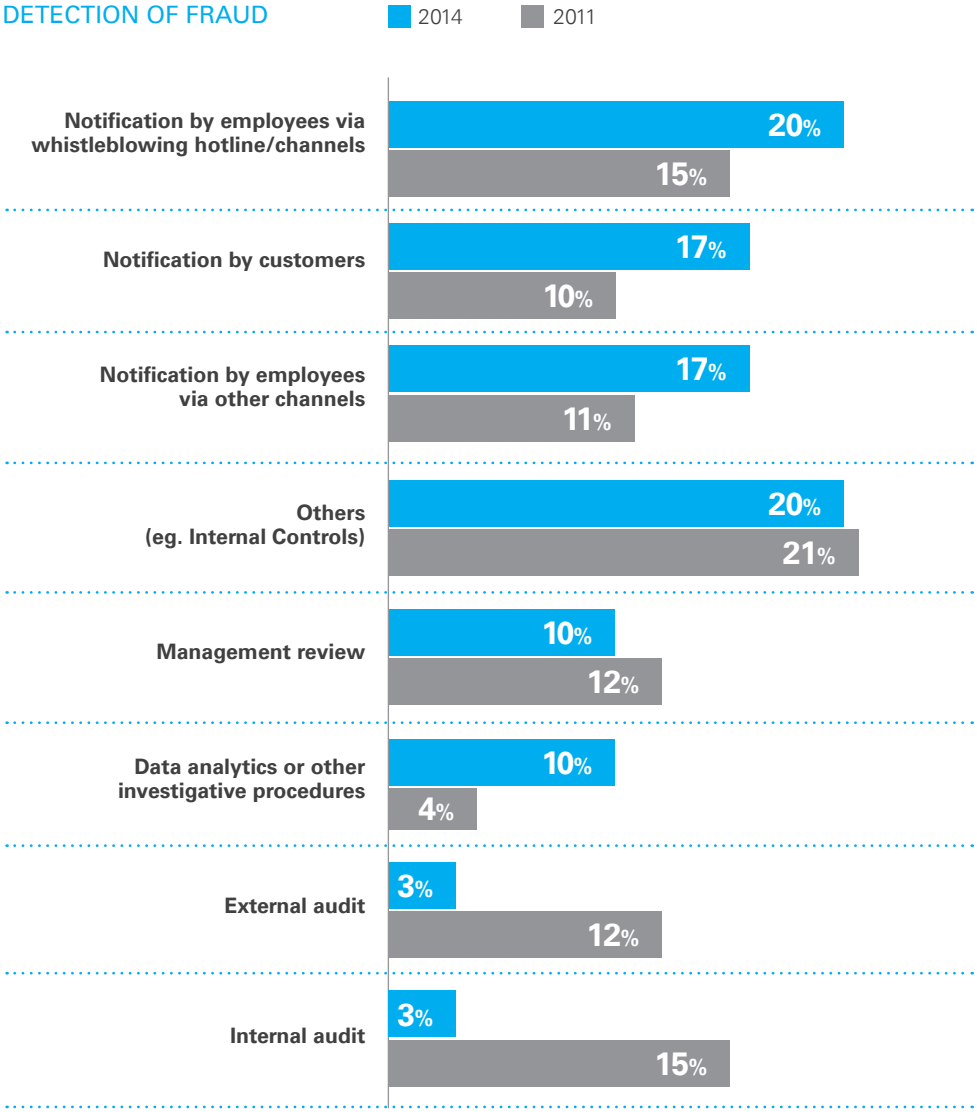
Also critical is establishing reporting channels where actual or suspected fraud can be reported in confidence and without fear of reprisal.

Just as vital is the need to train employees and external parties on how to make use of these channels.

The results confirm that fraud is best prevented on the "front line", i.e. by employees and management. Audit plays a valuable role in assessing the effectiveness of internal controls. However, when fraud occurs, internal and external audit take place after the event, by which time losses have already been incurred and may still be mounting.

The responses highlight how important it is for companies to develop and implement robust preventative measures to mitigate the risk of fraud.

DETECTION OF FRAUD



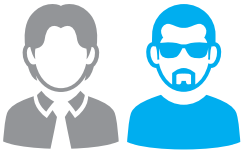
D. FACTORS CONTRIBUTING TO FRAUD

The survey results suggest that a combination of weak or overridden internal controls was the leading cause of fraud, identified by more than half (53%) the respondents.

53%

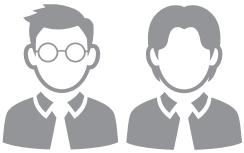
identified weak or overridden internal controls as the leading enabler of fraud

Collusion is another significant concern. Almost half the respondents said collusion between employees and third parties (30%) or collusion among employees (17%) enabled fraud to occur.



30%

cited collusion between employees and third parties



17%

cited collusion between employees

Fraud prevention measures can be improved. For example, 17% of respondents said the lack of employee or management familiarity with the 'red flags' of fraud allowed fraud to occur while 7% attributed it to weakness in management or board oversight. It is also a concern that 13% cited the ethical climate in an affected department or the organisation as a key factor.

Companies should reduce their exposure to fraud risk by reviewing the effectiveness of fraud prevention measures and educating employees and management about the risks in their business environment.

COMMENT

Fraud and misconduct are perpetrated by people. No one can anticipate when an individual will succumb to temptation or coercion and commit fraud.

Collusion is of particular concern as internal controls rely on supervisor reviews and approvals, and third party documentation.

Control mechanisms, which may appear effective, can break down when operated by staff who collude with others.

Enforcement and accountability protocols need to be put in place to enforce disciplinary action and hold perpetrators accountable for their behaviour.

A company's approach to accountability, for instance, should include an understanding that it is the management's responsibility to manage fraud risk effectively.

Management must therefore ensure that it commits time to addressing the risks of fraud facing the organisation.

FACTORS THAT ENABLED FRAUD TO TAKE PLACE

53%

Weakness in internal controls or overridden controls

30%

Collusion between employees and third parties

17%

Collusion between employees

17%

Employee or management unfamiliarity with red flags of fraud

13%

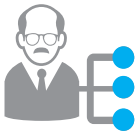
Ethical climate in affected department or organisation

7%

Weakness in physical security

7%

Weakness in IT security



7%

Weakness of management or board oversight

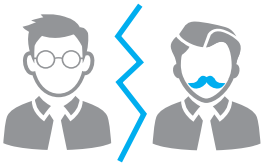
Percentages do not total 100% due to multiple response options

E. RESPONSE TO FRAUD

When fraud is suspected or confirmed, the most common company response is to carry out an internal investigation.

83 %

undertook an investigation of the incident



57 %

terminated relations with the perpetrator

Conducting an internal investigation was cited as the most common organisational response by 83% of respondents. This highlights the importance companies attach to determining the 'how, why, who, what and where' of any fraud incident.

The second most common response (57%) was to terminate relations with the perpetrator, whether this was an employee, vendor or business partner.

COMMENT

In addition to putting in place prevention and detection measures, companies should also implement protocols for response to actual or suspected fraud incidents.

The worst time to be making difficult decisions about the investigation processes, communication, or remediation around fraud is when an organisation is in the midst of an incident.

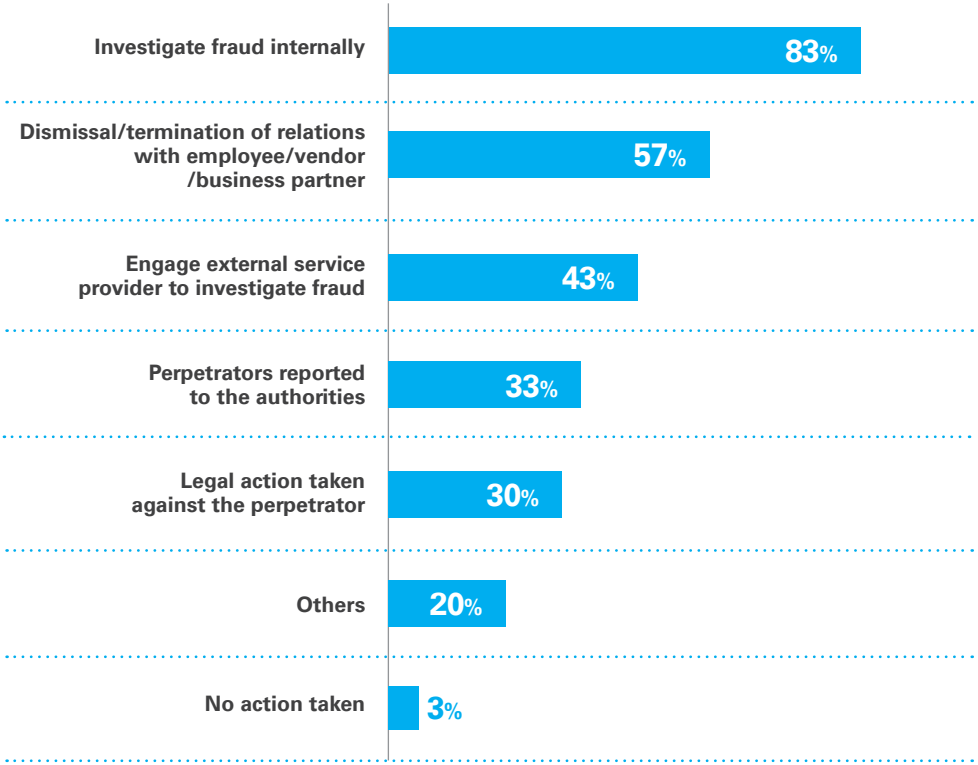
Protocols for managing actual or suspected fraud incidents should include:

- internal investigation processes and responsibilities
- corrective actions, such as internal control review and improvement
- enforcement of disciplinary actions and accountability of management and employees
- evaluation of what, how and when to communicate with stakeholders about the incident.

Interestingly, 43% of respondents stated that external parties were engaged to investigate when incidents occurred. Although there is a cost associated with such providers, the high degree of use of external parties may be a result of a number of factors, including:

- A need to ensure the objectivity of the investigation
- Having insufficient internal resources with the appropriate experience
- Needing access to specialised skills such as computer forensics or accounting
- Avoiding the accidental loss of the integrity of the evidence
- A lack of experience in managing issues involved in investigations, in particular those related to regulatory breaches.

ACTIONS TAKEN IN RESPONSE TO SUSPECTED OR CONFIRMED FRAUD



Percentages do not total 100% due to multiple response options

Beyond the immediate response to fraud, what is just as important are the lessons learnt.

80 %
implemented new controls or changed existing ones

Given the significance of weak or overridden controls, it is no surprise that implementing new controls or changing existing ones is the most commonly cited outcome.

37 %
implemented better communications

Implementing better communications was cited by 37% of respondents. This is valuable particularly if the incident provides 'teachable' lessons. Such communications should take into account relevant privacy and data protection laws.

OTHER ACTIONS TAKEN FOLLOWING THE CLOSURE OF FRAUD CASES INCLUDE:

13 %
Review of recruitment policies

13 %
Review of performance of person or committee in charge of fraud risk management

2 FRAUD RISK MANAGEMENT

A. FRAUD RISK MANAGEMENT PRACTICES ADOPTED

92%
said their company had a code of conduct

94%
said there was an appropriate tone set by management

Over nine out of ten respondents said their company had a code of conduct, with management setting an appropriate tone to encourage an ethical working environment.

According to 83% of the respondents, they have a person or committee tasked with managing fraud incidents.

While most companies have the cornerstones of fraud risk management in place, advanced anti-fraud measures were less prevalent.

For example, among respondents, only
- 75% said their company regularly assessed the likelihood and significance of fraud risks
- 65% said department managers participate in their departments' fraud risk assessments.

When taken in the context of the findings from Section 1, where over half the respondents identified weak internal controls or overridden controls as the largest cause of fraud, a clear picture emerges. Companies in Singapore need to pay more attention to implementing anti-fraud policies.

CORNERSTONES OF FRAUD RISK MANAGEMENT

	YES	IN PROGRESS /PLANNED	NO	NOT SURE
Is there a person or a committee in your organisation responsible for managing fraud incidents?	83%	5%	10%	2%
Does the organisation have a code of conduct in place?	92%	5%	3%	0%
Is there an appropriate tone from management which encourages a sound and ethical working environment?	94%	2%	1%	3%

FRAUD RISK MANAGEMENT PRACTICES ADOPTED

	YES	IN PROGRESS /PLANNED	NO	NOT SURE
Are there controls to detect potential or actual fraud in your organisation?	92%	5%	2%	1%
Does management attempt to identify possible fraud risks for their organisation/industry?	83%	9%	7%	1%
Are there controls to detect actual or potential frauds in your organisation?	81%	10%	7%	2%
Does the management assess the likelihood and significance of the possible fraud risks regularly?	75%	9%	10%	6%
Do individual department managers participate in the identification of possible fraud risks in their departments?	65%	5%	25%	5%

Of the respondents surveyed, 85% said their company communicates its fraud and ethics policies internally demonstrating understanding that employees are the first line of defence against fraud.

However, with only 59% of respondents saying that their employees are well informed about fraud risk, internal communication can surely be improved.

85%

indicated that their company communicates its fraud and ethics policies internally

59%

indicated that their employees are well informed about fraud risk

In addition, while 91% of respondents were very or somewhat concerned about the conduct of third parties (see Section 3: Cross-Border Activity) only 41% said their company communicates its fraud and ethics policies externally to third parties such as suppliers and business partners.

COMMENT

Organisations should periodically monitor the effectiveness of anti-fraud policies across their organisation.

Monitoring plans should encompass activities that are tailored to the nature and degree of the risk involved.

Where third parties are involved and greater risks may be faced:

- conduct due diligence/ integrity checks (periodically as well as at onboarding)
- include 'right to audit' clauses in relevant contracts and exercise those rights on a risk-based approach
- communicate anti-bribery and corruption policies, including contract clauses (e.g. the ICC Anti-corruption Clause).

COMMUNICATION AND TRAINING

	YES	IN PROGRESS /PLANNED	NO	NOT SURE
Are fraud and ethics policies communicated internally to all employees?	85%	6%	6%	3%
Are employees well-informed of the ways in which fraud can occur in your organisation?	59%	17%	15%	9%
Are fraud and ethics policies communicated externally (e.g. to suppliers, vendors) ?	41%	8%	40%	11%

B. EFFECTIVENESS OF ANTI-FRAUD MEASURES

The inescapable reality is that fraud continues to happen, even with most companies having some anti-fraud measures in place.

Having controls is important, but ensuring they are well designed, properly communicated, and consistently monitored and enforced is crucial to how effective they will be.

58%

said their company management monitors fraud risk indicators to pre-empt fraudulent activity

While it is positive that 58% of respondents said their company management monitors fraud risk indicators to pre-empt fraudulent activity, much more can be done to manage fraud risk and proactively boost the effectiveness of existing controls.

There is also room to improve how anti-fraud measures are reviewed and adjusted. Only 78% of respondents said their company reviews the effectiveness of its control measures regularly, and just 74% do so after each fraud incident.

COMMENT

Organisations can deploy sophisticated anti-fraud data analytics to help detect fraud and misconduct as well as to understand the root causes of irregularities.

More sophisticated predictive analytic tools employ an array of statistical techniques and modelling to analyse current and historical information to make predictions about potential weaknesses to fraud.

Such predictions can support fraud prevention, detection and response strategies by identifying control vulnerabilities, fraudulent transactions in real time, and potential suspects during investigations.

ANTI-FRAUD MEASURES AND FRAUD RISK INDICATORS

	YES	IN PROGRESS /PLANNED	NO	NOT SURE
Does management review the effectiveness of control measures on a regular basis?	78%	8%	10%	4%
Does management review effectiveness of control measures after each fraud incident?	74%	8%	4%	14%
Does management monitor various fraud risk indicators (e.g. unusual spikes in sales numbers, high turnover rate of key personnel) to pre-empt fraudulent activities?	58%	13%	17%	12%

3 CROSS-BORDER ACTIVITY

A. CONCERNS WHEN DOING BUSINESS OUTSIDE OF SINGAPORE

Growing regional integration and economic growth are creating ever more business opportunities in ASEAN (Association of Southeast Asian Nations) member countries.

While Singapore ranks among the five least corrupt nations in the *Transparency International Corruption Perceptions Index 2013*, standards across the region vary due to differing local business practices and industry norms.

66%

felt the risk of bribery and corruption was a key concern for Singapore companies conducting business in the region

Most respondents (66%) felt the risk of bribery and corruption was a key concern for Singapore companies conducting business in the region.

51%

were concerned about the need to provide payments or gifts in order to win or retain business

vs 20% in 2011

This risk can take many forms. For example, a growing worry for companies is the need to provide payments or gifts in order to win or retain business. Findings indicate that 51% of respondents were very concerned about this issue, up from 20% in 2011.

Foreign government officials and overseas-based third parties were also causes of concern for more than one-third of respondents. A considerable proportion (43%) reported being very concerned about interacting with foreign governments, and 36% were very concerned about using third parties.

COMMENT

When doing business abroad, companies need to undertake risk assessment procedures to understand and prepare for potential risks.

They should carry out due diligence to understand who they are working with and who will be conducting business on their behalf.

One approach is to develop formal processes for identifying and assessing potential risks in new territories that a company intends to enter.

These assessments typically include reviewing relevant business factors such as:

- the risks inherent to the new jurisdictions
- the nature of contractual relationships
- government relationships
- cultural norms and differences in those jurisdictions, as well as any relevant laws and regulations
- reliance on agents.

These processes should be refreshed periodically, or during major changes to business operations.

In addition, in-country personnel should be educated on such risks and how to manage them.

CONCERNS REGARDING RISKS WHEN DOING BUSINESS OUTSIDE SINGAPORE

	VERY CONCERNED	SOMEWHAT CONCERNED	NOT CONCERNED
Bribery and corruption	66%	29%	5%
Payments or gifts to win or retain business	51%	39%	10%
Unusual industry norms and/or business practices	46%	48%	6%
Interaction with foreign governments	43%	47%	10%
Use of third parties	36%	55%	9%

B. MITIGATING CROSS-BORDER RISKS

Respondents reported a variety of approaches used by their organisations to mitigate risks in cross-border activities:

78%
reported that employees were issued guidelines for mitigating cross-border risks

66%
of the organisations surveyed had established compliance programmes in place

61%
conducted training for staff

Just 48% of respondents reported that their organisation would forfeit a business opportunity, if necessary, to avoid fraud or corruption risks.

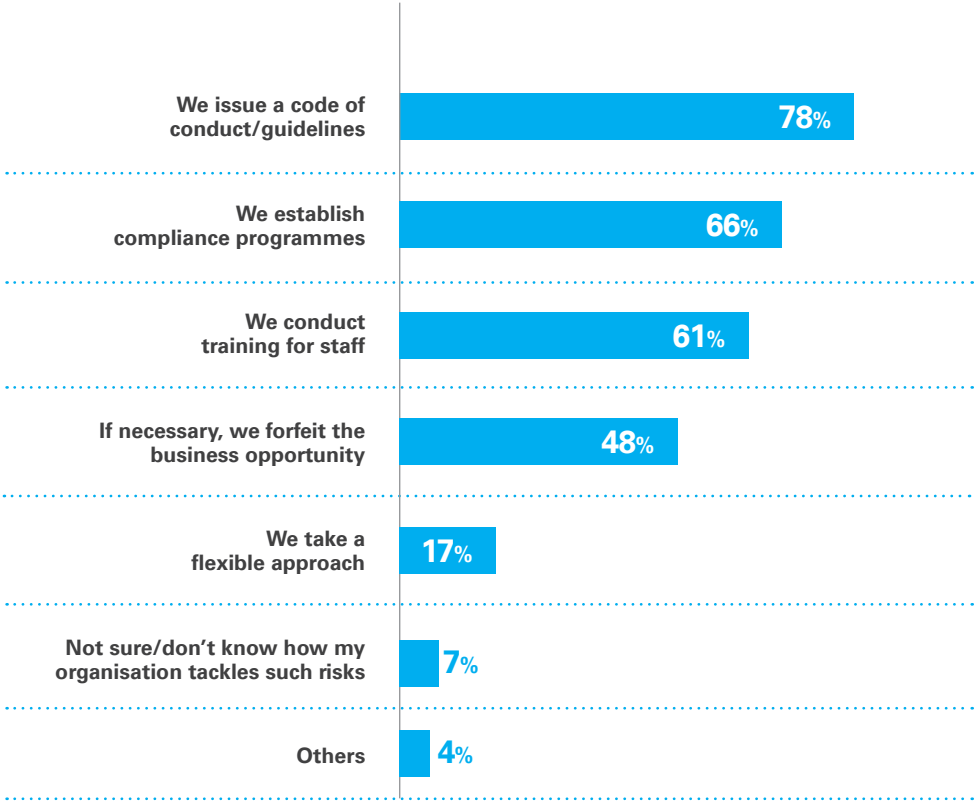
COMMENT

Forfeiting a business opportunity may be the appropriate action if risks cannot be managed.

However, good risk management is not always about turning away business. It is about managing the risks and taking advantage of the opportunity consistently with the organisation's risk appetite and regulatory and social expectations.

By anticipating and mitigating corruption risks, companies can turn good risk management into competitive advantage.

APPROACHES TO MITIGATING CROSS-BORDER RISKS



Percentages do not total 100% due to multiple response options

4 E-CRIME

A. CONCERNS ABOUT E-CRIME

E-crime is an emerging area of concern and tackling it is proving challenging in the absence of in-depth understanding of how e-crime occurs and how it can be prevented.

The complexity and rapid evolution of technology also adds to the unease around employee behaviour and the risk of customer or business data being stolen, falsified or otherwise misused.

64%

were very concerned about employees misusing sensitive information

>50%

were very concerned about falsification and manipulation of company records, master data and/or electronic audit trails

50%

were very concerned about employees stealing company assets

using technology such as e-banking, indicating theft by electronic means is a growing worry (up from 30% in 2011).

COMMENT

These days, having IT security tools integrated into the organisation's technology architecture is essential. However, there is no substitute for a coherent cyber-security plan.

Understanding the trends in external threats and using this insight to formulate policy and strategy is critical to long-term incident prevention. This involves an analysis of external and internal threat patterns to understand the various cyber-crime risks, and the short, medium and long term implications for the organisation. Only then can a company anticipate cyber-threats. Monitoring of IT networks needs to be underpinned by such intelligence and can only be as effective as the company's knowledge of what to look for in its systems.

A framework to assess and report cyber-security risks has to be developed. As part of a wider enterprise risk management framework, strategic insight into cyber risks and the potential impact on the organisation's core business is paramount.

Knowledge and awareness among end users is similarly critical. Returns from investing in IT security tools are best provided by staff who understand their responsibilities for keeping their networks safe.

CONCERNS ABOUT E-CRIME

	VERY CONCERNED	SOMEWHAT CONCERNED	NOT CONCERNED
Misuse of sensitive information (e.g. customer or business data)	64%	33%	3%
Falsification of company records	59%	24%	17%
Manipulation of standing data (e.g. vendor master records)	52%	35%	13%
Manipulation of electronic audit trails	51%	34%	15%
Theft of company assets through electronic means (e.g. e-banking, e-wallet)	51%	26%	23%
Downloading/installing unauthorised software	44%	42%	14%
Social media (e.g. Twitter, LinkedIn, Facebook)	29%	53%	18%

B. PERCEIVED WEAKNESS IN IT INFRASTRUCTURE

20%

were completely satisfied with how their organisations defend themselves against e-crime

As only one in five respondents were completely satisfied with their organisation's e-crime defences, more can clearly be done to improve IT safeguards in terms of software, hardware or procedures.

COMMENT

This finding is another indication that companies should strengthen their procedures for fraud risk assessment **(see Section 1D: Factors contributing to fraud)**, and should include IT infrastructure as part of this assessment.

In addition, employees' fraud awareness training should include information on the risks involved in storing data on portable storage devices and the benefits of encrypting documentation, where applicable.

HOW SATISFIED ARE YOU WITH YOUR ORGANISATION'S LEVEL OF SECURITY AGAINST E-CRIME?

	2014	2011
Completely Satisfied	20%	17%
Somewhat Satisfied	74%	79%
Not Satisfied	6%	4%

Employee behaviour is of particular interest as a key area of weakness in their organisation's IT security.

56%

viewed employees' use of email as a major concern

54%

were very concerned about mobile data storage such as thumb drives

vs 32% in 2011

50%

were very concerned about smartphones and their potential to undermine the security of their business

vs 17% in 2011

84%

were somewhat or very concerned about the security implications of cloud storage

These findings underline the growing worry surrounding data storage and the means by which data can potentially be removed from internal networks. In the case of cloud storage, where documents and data are stored in external data centres, offsite and third party security is a substantial concern.

PERCEIVED IT SECURITY RISKS

	VERY CONCERNED	SOMEWHAT CONCERNED	NOT CONCERNED
Employee email (e.g. leaking of confidential information)	56%	38%	6%
Mobile data storage (e.g. thumb drives or portable hard disk drives which are lost or used to remove company data)	54%	40%	6%
Smart phones (e.g. client or business data held on a lost phone or similar devices)	50%	42%	6%
Cloud storage	41%	43%	16%

CONCLUSION

Companies in Singapore realise that fraud is widespread and deserves close attention.

However, the increase in internal fraud since 2011 suggests that while many companies in Singapore already have anti-fraud controls in place, these controls are often inadequate. They may be dodged or overridden, or just poorly implemented or communicated.

Companies need to enhance the implementation of their anti-fraud policies, notably in the areas of:

- training and communication to develop awareness of fraud and the anti-fraud policies adopted by the organisation
- fraud risk assessment to proactively identify potential fraud risks and mitigate them before they become an incident
- ongoing monitoring of the effectiveness of anti-fraud measures
- enforcement and accountability protocols to enforce disciplinary action and hold management and perpetrators accountable for their behaviour.

Bribery and corruption are also concerns for companies operating outside Singapore for which more proactive measures are needed.

For example, conducting risk assessments to understand and prepare for bribery and corruption risks overseas can be helpful. It is also important to conduct due diligence on business partners and agents in those markets.

With e-crime on the rise, employee behaviour and the use of technology to commit fraud is increasingly the focus. It is therefore essential for companies to include IT as part of their risk assessments.

The overarching message is clear: much progress has been made, but more work is needed if corporate controls are to operate as a robust defence against fraud.

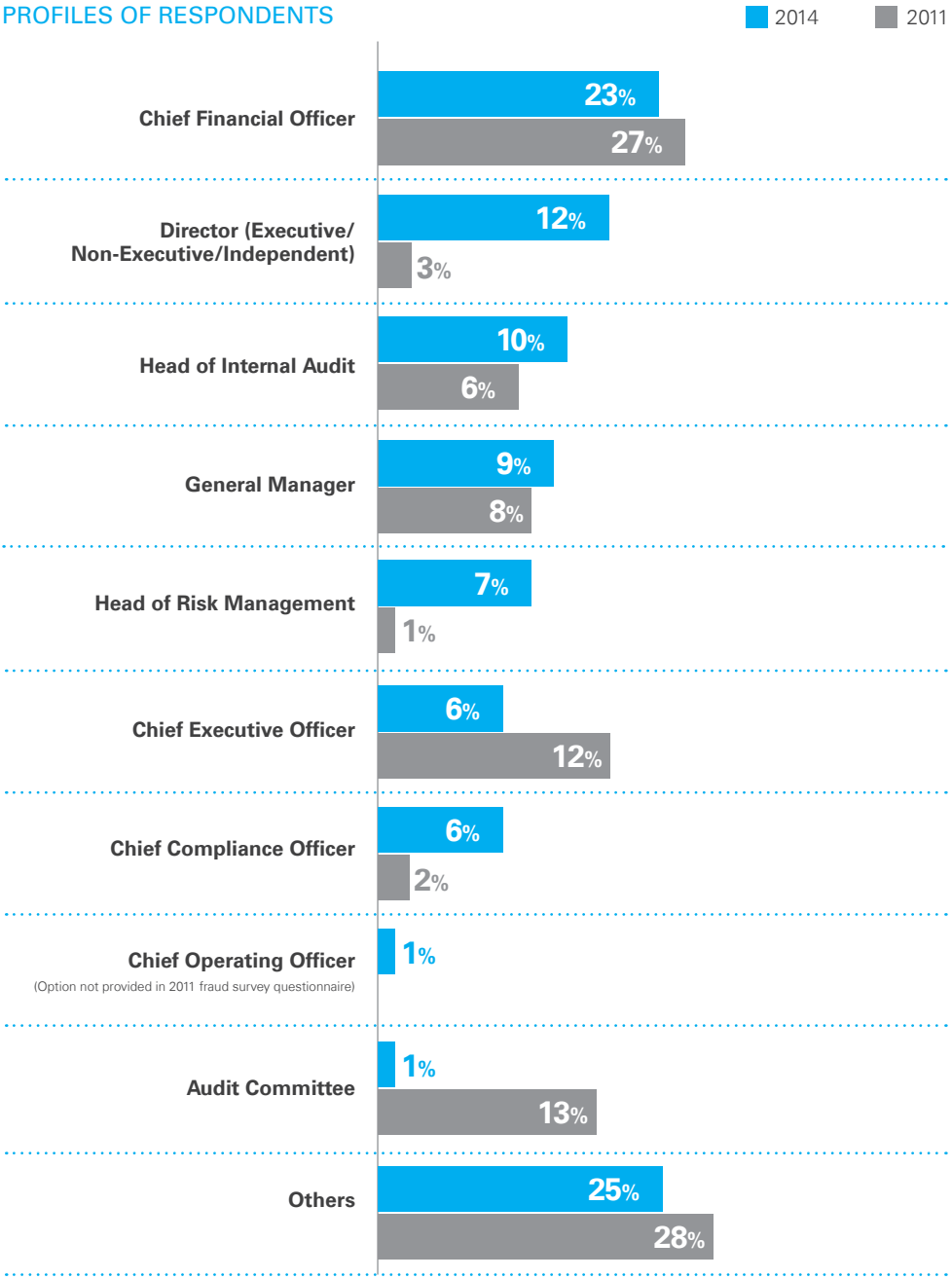
ABOUT THIS SURVEY

In the last quarter of 2013, KPMG, in collaboration with SMU, sent questionnaires to the top companies incorporated in Singapore and those listed on the Singapore Exchange.

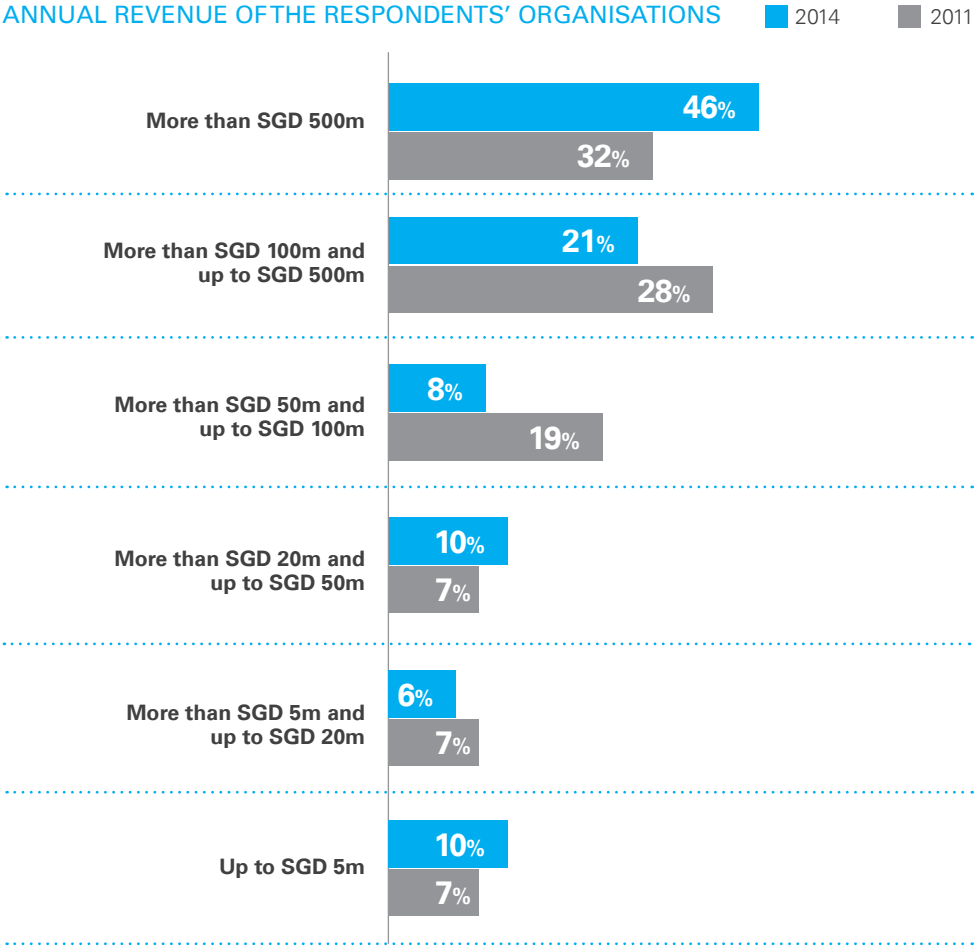
The survey received 103 responses from a broad range of industries. About 75% of these organisations had annual revenue exceeding S$50 million.

More than 40% of respondents were a chief executive officer, chief financial officer, audit committee member or board member in their organisation.

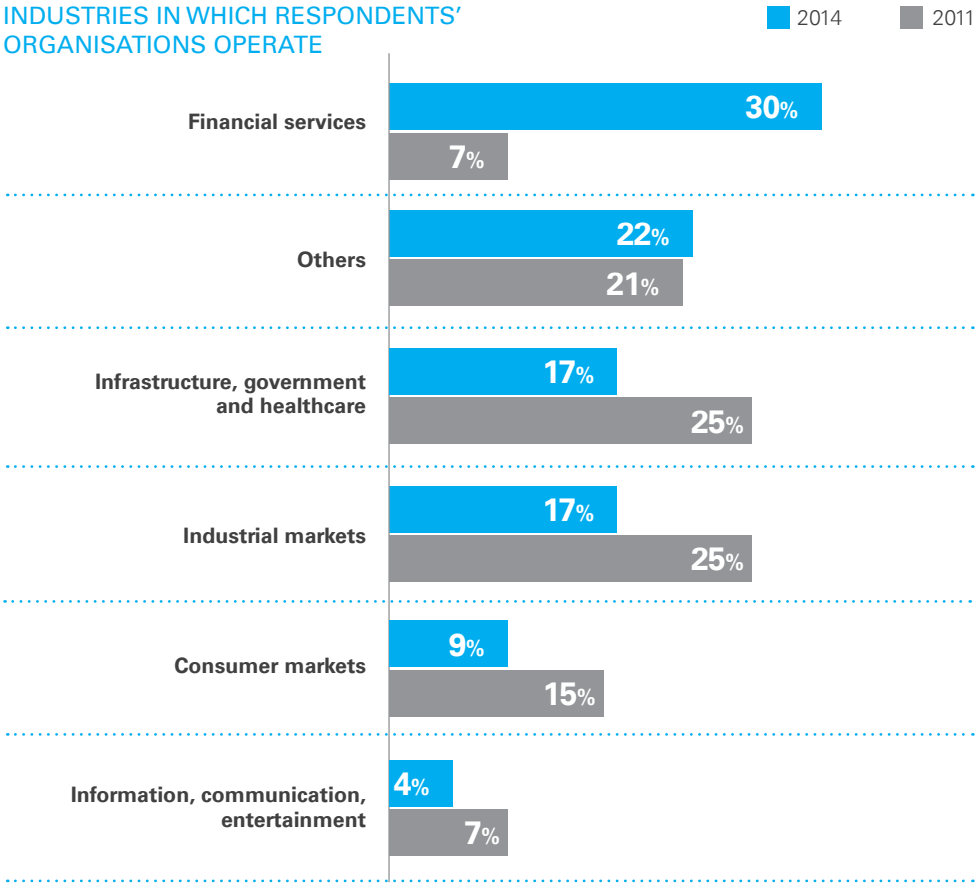
PROFILES OF RESPONDENTS



ANNUAL REVENUE OF THE RESPONDENTS' ORGANISATIONS



INDUSTRIES IN WHICH RESPONDENTS' ORGANISATIONS OPERATE



CONTRIBUTORS

PROF SEOW POH SUN
Associate Dean (Teaching & Curriculum),
Associate Professor of Accounting (Education)

PROF GARY PAN
Associate Dean (Student Matters),
Associate Professor of Accounting (Education)

PROF THEMIN SUWARDY
Associate Professor of Accounting (Practice),
Programme Director,
Master of Professional Accounting

CONTACT

BOB YAP
Head, Advisory
Tel: +65 6213 2677
byap@kpmg.com.sg

LEM CHIN KOK
Partner, Forensic
Tel: +65 6213 2495
clem@kpmg.com.sg

OWEN HAWKES
Partner, Forensic
Tel: +65 6213 2280
ohawkes@kpmg.com.sg

KPMG
16 Raffles Quay #22-00
Hong Leong Building
Singapore 048581
Tel: +65 6213 3388
Fax: +65 6225 0984

kpmg.com.sg