Global Economic Crime and Fraud Survey 2018:
Pulling fraud out of the shadows

Vietnam Perspectives
Foreword

PricewaterhouseCoopers Consulting (Vietnam) Ltd. (PwC) is proud to present its first-ever Global Economic Crime and Fraud Survey: Vietnam Perspectives.

Being a growing economy, Vietnam is attracting high levels of foreign direct investment. As often occurs in rapidly developing economies, anti-fraud measures may not develop at the same pace as the economy. Foreign investors, particularly those from developed economies, may not be prepared to face some of the difficulties that are present in such a dynamic, challenging environment. Hence, we see this present moment in Vietnam’s development as a relevant time to explore the insights from our survey relating to the economic crime landscape.

Respondents include personnel working in various roles, ranging from C-suite individuals to Internal Audit and Risk Management executives, representing companies from various industries, including key sectors of the Vietnamese economy such as Financial Services and Manufacturing. The ownership structure of these companies is diverse and includes publicly listed companies, private companies, and majority state-owned enterprises.
The key results from this survey are as follows:

- **52% of respondents report having suffered economic crime/fraud in the past two years**, a slightly higher incidence level than seen regionally (46% in Asia-Pacific) or globally (49%). Of those who reported being victims of fraud, the most common fraudulent activities were Asset Misappropriation, at 40%, and Bribery and Corruption, at 36%.

- **Culture trumps controls in Vietnam**: most fraudulent activities that were reported were identified through internal tip-offs (16%) or by accident (also 16%). However, Vietnam’s Internal Audit and whistleblowing hotlines each identified only 3% of the reported fraud, lagging far behind the Asia-Pacific and global statistics. At the global level, Internal Audit and whistleblowing hotlines were reported to have identified 14% and 7% of all fraud, respectively. At the Asia-Pacific level, the numbers were 18% and 7%, respectively. This is an area that Vietnamese companies could explore in order to mitigate the risks in achieving their strategic objectives.

- **Almost half of the Vietnamese respondents (47%) said they had been targeted by cybercrime in the previous two years**. However, only 12% of Vietnamese respondents predicted that cybercrime will have the most disruptive impact during the next two years. This accounts for almost a half of the global response rate (26%) and less than the regional response (21%). Given the relative early development state of its economy, 37% of the Vietnamese respondents advised that they: a) did not know whether they had a cybersecurity programme or not (16%); b) did not have such a programme (13%); or c) were only now assessing the feasibility of implementing such a programme (8%).

- **46% of the Vietnamese survey respondents have performed a general fraud risk assessment during the last two years**. However, fewer respondents have performed assessments that focus on specific risk areas, such as Anti-Bribery and Corruption (35%) or Cyber-Attack Vulnerability (29%). These statistics may increase in the future, given that 39% of the Vietnamese survey respondents reported having been asked to pay a bribe.

We hope this report will provide you with some interesting insights into Vietnam’s economic crime landscape and prompt you to start thinking about how to defend your business against the threats identified in this report.
About the survey

PwC’s 2018 Global Economic Crime and Fraud Survey was completed by 7,228 respondents from 123 territories. Of the total number of respondents, 52% were senior executives of their respective organisations, 42% represented publicly-listed companies and 55% represented organisations with more than 1,000 employees.
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview of fraud and economic crime in Vietnam</td>
<td>6</td>
</tr>
<tr>
<td>A transparent picture</td>
<td></td>
</tr>
<tr>
<td>Organisational damage</td>
<td></td>
</tr>
<tr>
<td><strong>Profile of perpetrators</strong></td>
<td>10</td>
</tr>
<tr>
<td>Who are the fraudsters?</td>
<td></td>
</tr>
<tr>
<td>How are fraudsters detected?</td>
<td></td>
</tr>
<tr>
<td>How do companies deal with fraudsters?</td>
<td></td>
</tr>
<tr>
<td><strong>Business ethics and compliance</strong></td>
<td>14</td>
</tr>
<tr>
<td>How are these programmes operated?</td>
<td></td>
</tr>
<tr>
<td>How can we improve the programme?</td>
<td></td>
</tr>
<tr>
<td><strong>Anti-money laundering</strong></td>
<td>18</td>
</tr>
<tr>
<td>What is happening in Vietnam?</td>
<td></td>
</tr>
<tr>
<td>The roles of Vietnam Government and State Bank of Vietnam</td>
<td></td>
</tr>
<tr>
<td><strong>New disruptive technologies</strong></td>
<td>21</td>
</tr>
<tr>
<td>Is Vietnam lagging behind?</td>
<td></td>
</tr>
<tr>
<td>Cyber response plans</td>
<td></td>
</tr>
</tbody>
</table>
Overview of fraud and economic crime in Vietnam
A transparent picture

Our survey indicates that companies in Vietnam have experienced a fraud rate of 52% during the last two years, a figure that is slightly higher than in the Asia-Pacific region or at the Global level, which stand at 46% and 49%, respectively.

However, given our experience with fraud, we suspect that the 40% of respondents who advised that they did not experience fraud may simply not have detected it as yet.

Economic crime comes in many forms, each with a different nature. The most common types of economic crime reported by respondents was Asset Misappropriation (40%) and Bribery and Corruption (36%). The figures for both of these crimes are higher than the corresponding Asia-Pacific and global figures. Surprisingly, only 7% of the respondents believe that Asset Misappropriation will reoccur in the next 24 months, while Bribery and Corruption is predicted to reoccur by 27% of respondents.

Is the risk of Asset Misappropriation underestimated? Or do Vietnamese companies have an insufficient level of awareness of risks associated with this type of fraud, despite the fact that incidence levels have risen considerably?

Types of fraud experienced in past 24 months

- Asset misappropriation: 40%
- Bribery and Corruption: 36%
- Procurement Fraud: 29%
- Accounting Fraud: 24%
- Business Conduct/Misconduct: 22%
- Fraud committed by consumers: 20%
- Cybercrime: 16%
- Human Resources Fraud: 16%
- Money laundering: 13%
- Tax Fraud: 9%
- Insider Trading: 7%
- Intellectual Property (IP) theft: 7%
- Competition/Anti-Trust Law Infringement: 7%
- Other: 7%

Don’t know: 8%
Vietnam has the highest Asset Misappropriation rate compared to Japan and Korea.

As shown in the graphic below, as compared to Vietnam’s major trading partners, Japan and Korea, Vietnam (40%) leads the group for Asset Misappropriation. However, in terms of Bribery and Corruption amongst the trading partners, Korea leads (42%), followed by Vietnam (36%), and then Japan (12%). These results may provide some level of insight into the respective priorities of the anti-fraud programmes in the countries specified.

**Top two fraud types compared to Korea and Japan**

- **Vietnam**: 40% Asset misappropriation, 36% Bribery and Corruption
- **Korea**: 38% Asset misappropriation, 42% Bribery and Corruption
- **Japan**: 22% Asset misappropriation, 12% Bribery and Corruption
Organisational damage

Damages from economic crimes can be classified into financial and non-financial types. There are several types of quantifiable financial consequences of fraud, including remediation costs, legal fees, actual monetary losses, and even criminal penalties, for example. However, despite the fact that non-financial damages may not be quantifiable, they can lead to potentially worse consequences than financial losses (i.e. reputational damage, employee morale).

<table>
<thead>
<tr>
<th>Financial damage reported</th>
</tr>
</thead>
<tbody>
<tr>
<td>Don’t know</td>
</tr>
<tr>
<td>Amount is immeasurable</td>
</tr>
<tr>
<td>5 million to &lt; 50 million US dollars</td>
</tr>
<tr>
<td>1 million to &lt; 5 million US dollars</td>
</tr>
<tr>
<td>100,000 to &lt; 1 million US dollars</td>
</tr>
<tr>
<td>50,000 to &lt; 100,000 US dollars</td>
</tr>
<tr>
<td>25,000 to &lt; 50,000 US dollars</td>
</tr>
<tr>
<td>Less than 25,000 US dollars</td>
</tr>
</tbody>
</table>

On one hand, our survey measured the damage from economic crimes in terms of its pure financial impact on Vietnamese organisations. 53% of the Vietnamese companies in our survey reported losses of less than $100,000 (approximately VND2.3 billion) as a result of economic crimes over the last two years. Just under one-third of the Vietnamese survey respondents (32%) estimated they lost more than $100,000 to fraud in the same period.

On the other hand, non-financial impact was also measured in our survey. The most severe impact the Vietnamese survey respondents identified was to their reputation/brand strength (28%). This was followed by the impact on employee morale and business relations, where 23% and 21% of respondents felt the greatest impact, respectively.

Surprisingly, six out of every ten respondents advised that economic crime had no effect on their share price.
Profile of perpetrators
Who are the fraudsters?

In Vietnam, the majority (53%) of reported economic crime is perpetrated by internal actors. The percentage of reported frauds that are carried out by external actors is 36%, by contrast, while 8% say they are unaware of the identity of fraudsters.

When it comes to internal actors, our survey reveals that Senior Management are reported to have committed 19% of internal fraud, while Junior Management are reported to have perpetrated 28%. However, the greatest perpetrators of internal fraud were reported to be Middle Management staff at 33% according to survey respondents.

Approximately 24% of respondents advised internal fraud was most likely to be committed by Marketing and Sales personnel. By contrast, at both the Asia-Pacific and global levels, most internal fraud reportedly was perpetrated by Operational and Production personnel.

In Vietnam, though, external threats are clearly substantial. These external actors include Customers (36%), Vendors (21%), and Agents, Hackers, and Organised Crime, at 14% each. We have termed the first three of these categories as “frenemies”. We believe this title is fitting for Southeast Asia, where relationships, related parties and potential conflicts of interest are a common and integral part of the business landscape.

Our respondents identified the main driver for fraud was “Opportunity” leading to economic crime (38%), followed by “Incentives and/or Pressure to Perform” (33%).
How do companies deal with fraudsters?

During the past two years, Vietnamese companies have purportedly undertaken fraud risk assessments on a regular basis – with just under half of respondents advising they had performed such an assessment (46%). However, 16% of respondents admitted that no assessments had been performed in the past 24 months. In addition, 15% of respondents weren’t sure whether they had performed any assessment (one can assume if you are unsure as to whether or not you have undertaken a fraud risk assessment, the odds are that it didn’t happen!).

We note companies worldwide are performing cyber risk assessments. In fact, Cyber-Attack Vulnerability was ranked as the second most important risk category, at 46% globally and 41% regionally. In Vietnam, however, it seems there is less concern regarding cyber risk, with only 29% of the respondents having performed a Cyber-Attack Vulnerability assessment.
Similar to companies around the globe and in the Asia Pacific region, Vietnamese organisations are investing in improving their business processes in order to combat fraud. 42% of respondents rate their level of effort in this area as “high”. Fewer, however, are putting the same level of effort into other anti-fraud efforts, such as promoting and verifying ethical decision making by individual employees. Again, this is a potential area for improvement for Vietnamese companies and also presents a major challenge to educate employees of the potential wider impact their decisions have on the organisation.
Business ethics and compliance
Approximately 64% of the respondents in Vietnam believe a formal business ethics and compliance programme is an urgent need for an organisation. This lags behind the Asia-Pacific region by 10%, and by 13% against global survey respondents, where 77% of respondents advised they already have implemented a formal Ethics and Compliance programme.

We anticipate Vietnamese companies will increase the adoption of these programmes in the near future, as they will not only be expected by local regulatory bodies, but also multinational partners and foreign investors. Early adoption of Ethics and Compliance programmes by Vietnamese companies increases their attractiveness to business partners and investors, which is critical for future growth prospects.

Unfortunately, our survey also indicates Vietnam is following a disturbing global and regional trend in that 39% of respondents advise they have been requested to pay bribes. The global rate of bribe requests is 23% in the current survey, which is 6% lower than the rate in the Asia-Pacific region.

Of the respondents in Vietnam, 30% believe they have lost opportunities to competitors who have paid a bribe. However, approximately 42% of Vietnamese organisations do not possess any knowledge about the rival that purportedly benefited from the bribe.
Who has primary responsibility for the business ethics and compliance program in your organisation?

Unlike their overseas counterparts, 18% of the companies in Vietnam say their Chief Risk Officer (CRO) is responsible for the Ethics and Compliance programme, in addition to other management officers including Chief Executive Officer (CEO) and the Chief Compliance Officer (CCO). By contrast, the roles of General Counsel, Chief Audit Officer (CAE), Chief Operation Officer (COO) and Chief Finance Officer (CFO) tend not to include responsibility for Ethics and Compliance programmes. Roughly 6% of the respondents
in the region, and roughly 6% of those around the globe, indicated that their CFOs “owned” the Ethics and Compliance programme, yet no respondents advised this was the case in Vietnam.

The HR Director and the Chief Audit Executive (CAE) have the primary responsibility for the Ethics and Compliance programmes, but only 10% of the respondents tagged these functions as having ownership. Rather, the CEO and the CRO roles have picked up the job in 36% of the respondents’ organisations.

### How can we improve Ethics and Compliance programmes?

In anti-bribery circles in the Western world, regulators will compare business expenses for compliance to the budget for office supplies. Companies that spend more on office supplies than compliance may be seen as not being serious in their quest to be compliant. Companies should give serious consideration to the level of resources they allocate to preventing and detecting fraud in their organisations.

Thus, we asked survey respondents to gauge their level of compliance expenditure over time. 56% of survey participants in Vietnam claimed that they have invested roughly the same level of funds in combatting fraud over the last two years as in previous years. Only 42% expect the level to stay the same over the next 2 years, while almost half of the respondents (48%) expect either an increase or a significant increase in their expenditure, in order to combat fraud related issues within their organisations.

### Who is responsible for the business ethics and compliance program in your organisation in Vietnam?

<table>
<thead>
<tr>
<th>Role</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CCO</td>
<td>37%</td>
</tr>
<tr>
<td>General Counsel</td>
<td>4%</td>
</tr>
<tr>
<td>CEO</td>
<td>18%</td>
</tr>
<tr>
<td>CAE</td>
<td>4%</td>
</tr>
<tr>
<td>CRO</td>
<td>18%</td>
</tr>
<tr>
<td>COO</td>
<td>2%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>9%</td>
</tr>
<tr>
<td>Other</td>
<td>2%</td>
</tr>
<tr>
<td>HR Director</td>
<td>6%</td>
</tr>
<tr>
<td>CFO</td>
<td>0%</td>
</tr>
</tbody>
</table>

### Anti-fraud investment level

<table>
<thead>
<tr>
<th>Period</th>
<th>Significant increase</th>
<th>Some increase</th>
<th>About the same level</th>
<th>Decrease</th>
</tr>
</thead>
<tbody>
<tr>
<td>In the past 24 months</td>
<td>11%</td>
<td>5%</td>
<td>56%</td>
<td>3%</td>
</tr>
<tr>
<td>In the next 24 months</td>
<td>17%</td>
<td>42%</td>
<td>31%</td>
<td>10%</td>
</tr>
</tbody>
</table>
Anti-money laundering
What is happening in Vietnam?

Money laundering is a global concern. Vietnam, being a largely cash-based economy, is considered a prime target for money laundering criminals, as cash leaves no audit trail. Encouragingly, Vietnamese organisations appear to be aware of AML regulations, as 86% of the respondents reported that their organisations are subject to AML regulations.

As with cyber threats and all fraudulent activity, it is preferable to prevent money laundering, rather than to “cure” after the fact. The 2018 survey suggests that Vietnam actually has a markedly higher rate of organisations that conduct the Anti-Money Laundering and Combat Financing of Terrorism (75%) assessments than at the global (62%) or Asia-Pacific (61%) levels.
The roles of Vietnam Government and State Bank of Vietnam (SBV)

Money laundering has been officially classified as a crime through the Vietnam Penal Code since July 2000. The Penal Code insofar as it relates to money laundering has been amended and superseded on two further occasions - July 2016 and January 2018. The Vietnamese Government and the State Bank of Vietnam have also implemented a number of regulations relating to money laundering including regulations relating to threshold reporting values.
New disruptive technologies
Is Vietnam lagging behind?

Digital technologies are reshaping the way that work is done. As it might be expected, economic criminals and fraudsters are also using technology to enable crimes.

In Vietnam, 12% of the respondents believe this type of crime is likely to have the most disruptive impact upon their organisation in the next two years. This accounts for almost half in comparison to the global response rate (26%) and less than the regional response (21%). We note these statistics indicate that cybercrime is perceived as an emerging threat to businesses in Vietnam.

Our 2018 GECS survey – Vietnam perspectives highlights almost half of all respondents in Vietnam (47%) have been targeted by cyber-attacks during the last 2 years. These respondents reported the most common method of cyber-attack was through Malware (the insertion of malicious software into the devices of the victims), which accounted for 23% of all incidences. Phishing, the use of e-mails to deceive recipients into divulging sensitive information, followed at 17%. More sophisticated or resource-intensive types of attacks, like “Man in the Middle” (intercepting sensitive information by misrepresentation) and brute force, appear to be less prevalent in Vietnam.
As with all fraud-related statistics, these are also subject to interpretation – for the 15% who ‘don’t know’, or the 38% who said they were not subject to a cyber-attack, is that really the case? Or could it simply be they have not yet detected the attacks to which they may have fallen victim? This is one of the many reasons we recommend undertaking periodic preventative risk assessments – to identify vulnerabilities before disaster strikes.

We also recommend to our clients they take advantage of the capabilities of technology in order to detect and monitor economic crime. Technological tools have become more powerful and less expensive, some even freely available to users in a limited/reader format. However, we note the Vietnamese respondents lag well behind the rest of the world when it comes to using certain key technologies to protect themselves by detecting fraud. For example, 75% of the respondents in Vietnam (in contrast to only 48% of respondents globally) don’t know if they use or do not use technology to perform Third-Party Due Diligence on their business partners. In today’s business world, it is not just a regulatory expectation but a key requirement of compliance to understand your business partners reputation. Automated due diligence systems can help to protect companies in the event their prospective business partners have a poor reputation (or no reputation), or are linked to potentially corrupt or otherwise criminal behaviour, or an extensive litigation history.

Similarly, in terms of general fraud detection, 57% of the survey respondents in Vietnam either don’t know if they use or do not use technology to monitor this risk. At the global level, by contrast, 62% of respondents utilise technology for fraud prevention. For Vietnamese companies, this is clearly an area that could be improved if fraud losses are reduced through relatively inexpensive monitoring technologies, resources, including cash and management time, can be utilised for more strategic items.
Cyber response plans

The 2018 GECS survey – Vietnam perspectives reveals that a large number of companies have an incident response plan for dealing with cyber-attacks. 62% of the respondents said they had either a ‘fully-in-operation’ or a ‘yes, but-not-yet-implemented’ plan in order to deal with cyber-attack issues.

Due to the nature of cybercrime, where methods of attack are relatively consistent, one of the best defenses is to keep informed regarding the latest threats and vulnerabilities. This, however, requires victims to share information about how they are being targeted, either with law enforcement, private cybersecurity specialists, or both. Amongst our survey respondents, however, only one third advised they would be likely to share information regarding potential cyber-attacks with government/law enforcement agencies. Another 28% said that they did not know, while 21% were “on the fence” and could not say whether they would be likely to share information about cybercrimes.

### Availability of a Cybersecurity Programme

<table>
<thead>
<tr>
<th>%</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>53%</td>
<td>Yes, this plan is fully in operation</td>
</tr>
<tr>
<td>16%</td>
<td>Don’t know</td>
</tr>
<tr>
<td>13%</td>
<td>No, we do not have a plan</td>
</tr>
<tr>
<td>9%</td>
<td>Yes, but it has not been implemented yet</td>
</tr>
<tr>
<td>8%</td>
<td>No, but we are currently assessing the feasibility of implementing such a plan</td>
</tr>
</tbody>
</table>

### Likelihood of sharing information

- Very unlikely: 5%
- Very likely: 23%
- Likely: 21%
- Neither likely nor unlikely: 12%
- Unlikely: 11%
- Don’t know: 28%
Of the 17% respondents who advised they would not share information regarding cybercrime, the three most common reasons provided include:

a) the risk of uncontrolled public disclosure;
b) they did not believe the law enforcement agencies possessed the expertise to assist; or

c) they did not trust the law enforcement agencies.

<table>
<thead>
<tr>
<th>Reason for not sharing information</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other</td>
<td>7%</td>
</tr>
<tr>
<td>Don’t trust the enforcement agencies</td>
<td>25%</td>
</tr>
<tr>
<td>Don’t believe that the law enforcement agencies have the required expertise</td>
<td>36%</td>
</tr>
<tr>
<td>Local law restricts the sharing of internal data</td>
<td>11%</td>
</tr>
<tr>
<td>Previous negative experiences</td>
<td>7%</td>
</tr>
<tr>
<td>Risk of liability for the crime</td>
<td>11%</td>
</tr>
<tr>
<td>Risk of uncontrolled public disclosure</td>
<td>32%</td>
</tr>
<tr>
<td>Legal privilege not to share</td>
<td>7%</td>
</tr>
<tr>
<td>May lead to additional regulatory enforcement action</td>
<td>14%</td>
</tr>
</tbody>
</table>
Conclusion

“Awareness, preparation and education are fundamental in preventing economic crime.”

Our survey indicates economic crime is a common problem facing businesses in Vietnam. Often, certain types of fraud (for example, procurement kickbacks) are considered as a cost of doing business, and as such, compliance and fraud risk management are perceived as low priorities for management. There is often a misconception that the costs of good governance outweigh the benefits, however as highlighted in this survey, fraud has not only financial but also non-financial impacts such as organization reputation and staff morale. Both of these impacts have lasting negative consequences for businesses. In weighing up the decision to be compliant companies must ask themselves, “What is the cost of doing the right thing?”

Therefore, when taking into account an organization’s strategic goals in any frontier or emerging market, we believe there are sufficient incentives for organizations to invest in fraud risk management, corporate governance and compliance. As the Vietnam becomes further integrated internationally, there will be an increasing need and obligation to adapt to international ethical and compliance standards, which are becoming a demand from international business partners and local regulators.

This survey highlights the challenges faced by respondents with respect to anti-bribery and anti-corruption where local business culture often clashes with western ideals and policies. However, as foreign investment continues to increase in Vietnam, local companies will be required to adapt to increasing standards in order to comply with anti-bribery and corruption regulations.

We recommend companies undertake regular training programs in order to communicate the importance of anti-bribery and anti-corruption policies to raise organizational awareness of the wider ramifications with respect to non-compliance regarding these policies. In addition, companies that decide to invest in anti-corruption and anti-bribery policy frameworks benefit by becoming more attractive from a foreign investor perspective.

Although, cyber risk mitigation appears to be a low priority for Vietnamese businesses. Perpetrators of cyber frauds tend to target and capitalise on countries and businesses that are not prepared or have little knowledge in this area. Therefore, it is important for country regulators and companies to maintain a level of awareness of potential cyber threats.

Given the number of companies that reported to be affected by economic crime and fraud, we recommend companies conduct periodic reviews of their potential exposure and develop and implement the appropriate frameworks, policies and procedures to protect themselves from potential financial and non-financial damages.
Contacts

Want to know more about what you can do in the fight against fraud?
Contact our experts

**Grant Dennis**  
**General Director**  
PricewaterhouseCoopers Consulting (Vietnam) Ltd.  
+84 903 749 806  
dennis.a.grant@pwc.com

**Alex Tan**  
**Partner**  
PwC Consulting Services (M) Sdn Bhd  
alex.tan@pwc.com

**Dinh Hong Hanh**  
**Partner**  
Financial Services Consulting  
PricewaterhouseCoopers Consulting (Vietnam) Ltd.  
+ 84 904 178 556  
dinh.hong.hanh@pwc.com

**Peter Viksnins**  
**Executive Director**  
PwC Consulting Services (M) Sdn Bhd  
pete.viksnins@pwc.com

**Francis Timings Sean**  
**Director**  
Forensics  
PwC Consulting Services (M) Sdn Bhd  
sean.timings@pwc.com

**Vo Tan Bich Ngoc**  
**Manager**  
Financial Services Consulting  
PricewaterhouseCoopers Consulting (Vietnam) Ltd.  
+84 909 129 316  
vo.tan.bich.ngoc@pwc.com

www.pwc.com/vn/crimesurvey-2018

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.
©2018 PricewaterhouseCoopers Consulting (Vietnam) Ltd. All rights reserved. PwC refers to the Vietnam member firm, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.