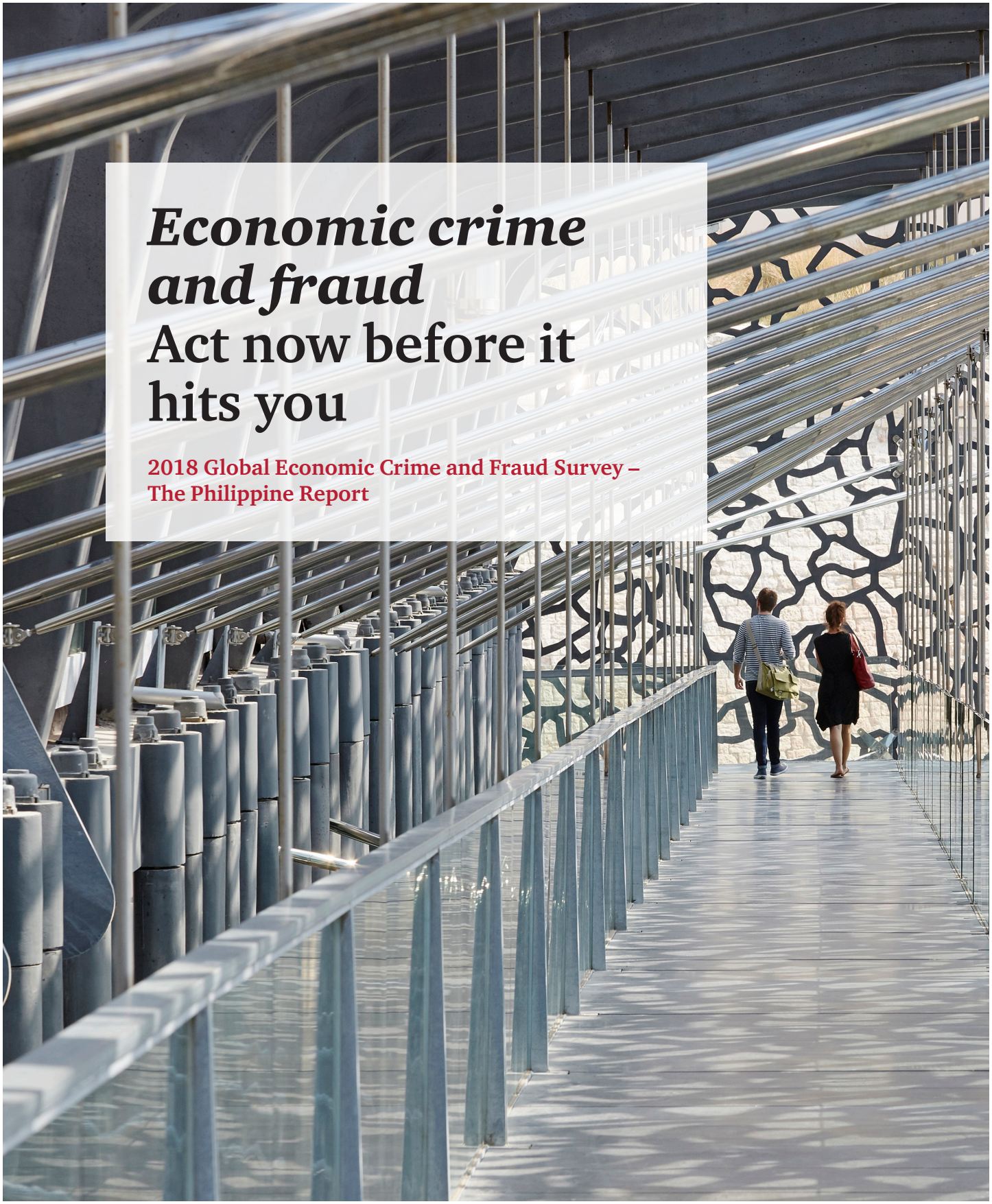
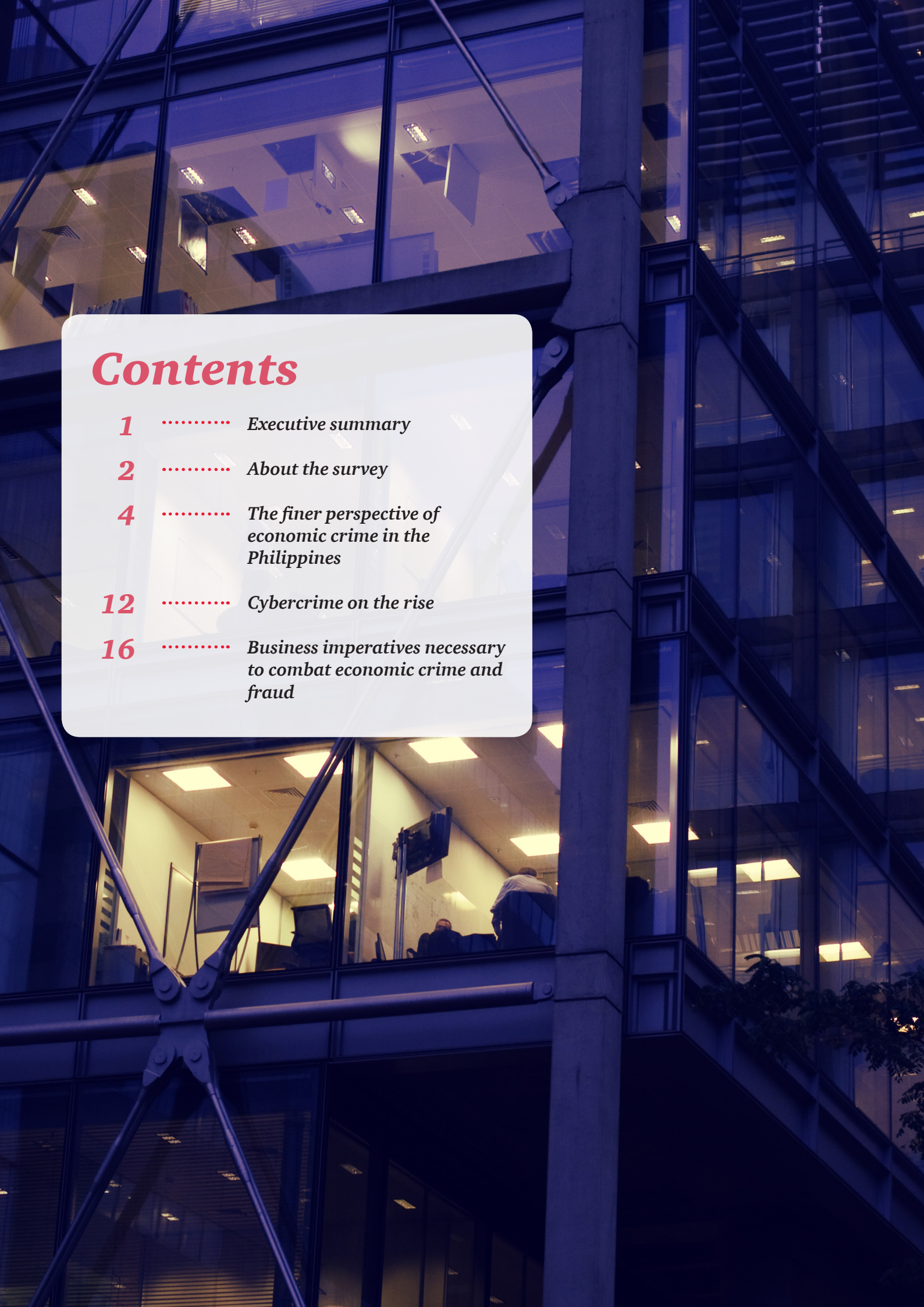


Economic crime and fraud Act now before it hits you

2018 Global Economic Crime and Fraud Survey – The Philippine Report

pwc

www.pwc.com/ph/fraudsurvey



Contents

A perfect storm of risks

In this era of unparalleled public scrutiny, today's organizations face a perfect storm of fraud-related risks – internal, external, regulatory, and reputational. The time is therefore right for them to adopt a new, more holistic view of fraud. It is one that recognizes the true steps of the threat: not merely a cost of doing business, but a shadow industry that can impact every territory, every sector, and every function. Since it hides in the shadows, a lack of fraud awareness within an organization is highly dangerous.

Didier Lavion
Principal, Advisory Forensic Services
Global Economic Crime and Fraud Survey Leader
PwC US

Excerpt from the PwC's 2018 Global Economic Crime and Fraud Survey (GECS) report

Foreword

PwC is privileged to present the Philippine report of the 2018 Global Economic Crime and Fraud Survey. This is the second local edition that is testament to the continued attention and focus of Philippine companies in addressing risks related to economic crime and fraud.

The global results indicate that fraud is at an all-time high, with 49% of respondents experiencing economic crime in the past two years. In a similar fashion, 54% of Philippine respondents confirm the same, and is higher than the 20% reported in 2016. These data may indicate two things: there is a general increase in the occurrence of economic crime, or organizations have become more aware and proactive in detecting and addressing economic crime than before.

The Philippines provides a diverse backdrop for organizations: a growing economy, evolving regulatory regime, coupled with varying business challenges and disruptive effects of emerging technology and innovation. This setting may have influenced the types of top economic crimes prevalent in local organizations, and can influence further the nature of what may come in the future. The pressure to perform and the available opportunities may have triggered more internal organizational actors to commit economic crime and fraud. With dependence on and integration of technology in organizations increasing more than ever, the related risk of cybercrime is on the uptick as well.

Despite these indicators that give a sneak preview of the local landscape, there is promise as Philippine organizations expressed optimism in their readiness to combat economic crimes in the next 24 months. Hopefully, this is not dampened by the less optimistic perspective on the impact of geopolitical environment.

Economic crime is a big issue to tackle on its own. However, organizational leaders should not lose sight of the overarching themes of corporate governance, risk management, and culture. Corporate leadership (board of directors and senior management) should set the tone, show by example, and place the controls for integrity and transparency in management and operations. In the process, ethical culture is strengthened and permeates all dealings and decision-making of all members of the organization. Lastly, everyone should have a strong risk consciousness to appropriately identify and manage the relevant economic crime and fraud risks.

We would like to thank all the Philippine companies who have responded to the survey. You have boldly contributed your insights and learnings to provide a snapshot of the corporate mindset and efforts in tackling fraud and economic crime locally. I enjoin everyone to take this report as the springboard for meaningful conversations and action plans on battling economic crime and fraud.

Roberto C. Bassig
Partner

Executive summary

In PwC's 2018 Global Economic Crime and Fraud Survey – The Philippine Report, one out of two (or 54%) of the respondents have indicated that their organizations have experienced economic crime and fraud at work. These anomalies, being obstinate threats, were experienced at work over the last 24 months. These affect both developed and emerging markets globally – the Philippines is not spared of this imminent threat.

Depending on the type of economic crime and fraud incident that organizations have experienced, the total impact of the incident threatens to further disrupt the organization's operations. Our study reveals that the incidents have high and medium impact on the employees' morale, followed by reputational/brand exposure, then relations with business partners and regulators.

Among the top five types of economic crime and fraud in the Philippines, asset misappropriation is still the most experienced type of incident. However, the most disruptive type of fraud in the Philippine workplace is consumer fraud. These disruptive incidents have been brought to the attention of Senior Management or Board Level Executives who are in charge of corporate governance. Businesses have lost approximately US$25,000 to US$100m due to these disruptive crimes.

Economic crime and fraud are no ordinary business issues due to certain anomalies committed by employees, management, and senior stakeholders of an organization. It is not acceptable that perpetrators are only removed from their positions. They should also be held accountable for all damages created by their anomalous schemes.

As part of an emerging market in the Asia Pacific region, Philippine businesses have a lot of things to do to improve its management control systems. By regularly conducting an enterprise-wide fraud risk assessment and responding to any reported fraudulent schemes in a timely manner will make a difference in the overall governance of the organization.

It may not be enough for organizations to invest in the latest technology available or to develop a robust anti-fraud framework. Rather, organizations should be investing in its people for them to be aware and to be equipped with necessary knowledge to combat fraud.

Organizations should also maintain an ethical culture, and observe appropriate corporate governance and accountability within the company. Understanding this principle not only gives senior management an opportunity to be a step ahead of fraudsters, but it also demonstrates positively to internal stakeholders that they are on top of corporate issues.

Economic crime and fraud are here to stay. Act now before it hits you.

About the survey

The 2018 Global Economic Crime and Fraud Survey (GECS) received valuable data from 7,228 respondents from 123 territories.

The aim of GECS is to assess:

- corporate attitude towards fraud and economic crime in the current economic environment
- the effect that these are having on organizations' business ethics and compliance programs
- what types of fraud are most common at work.

The Asia Pacific region had the most number of respondents globally at 31%, followed by Western Europe at 17%, then Eastern Europe and Africa regions at 14% each. Latin America had 12%, North America at 9%, and finally Middle East at 3%.

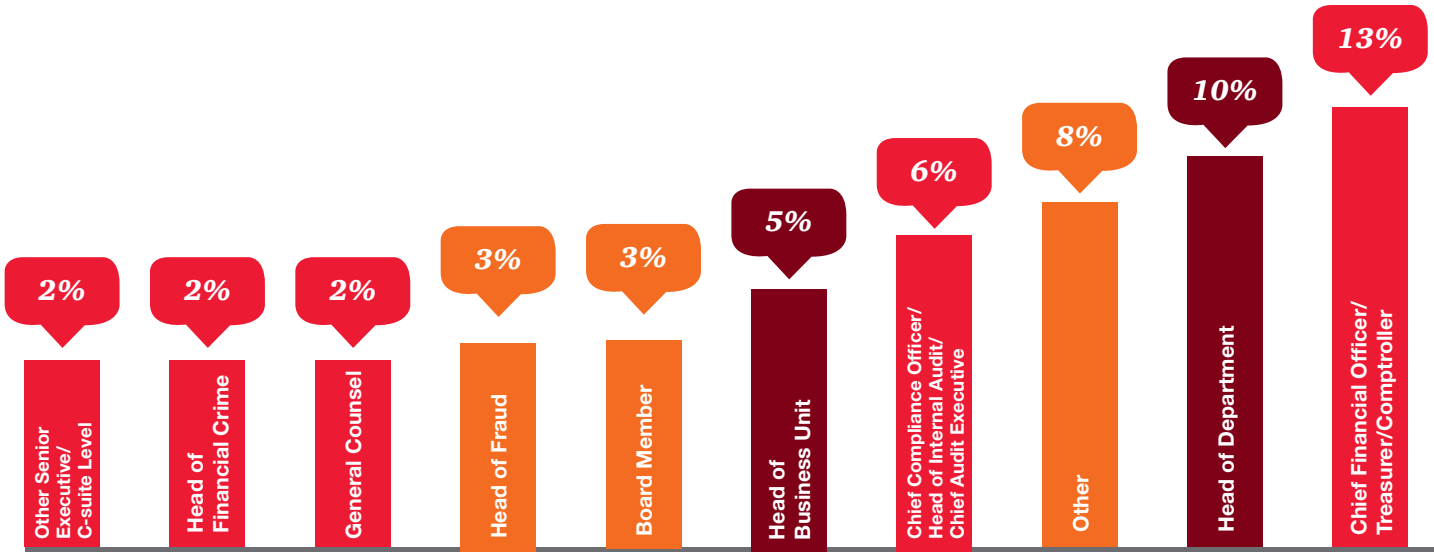
Approximately 5% of the total Asia Pacific respondents came from the Philippines.

The Philippine respondents' profile

There were 63 Philippine businesses who responded to this year's GECS who gave meaningful insights on economic crime and fraud incidents that they have encountered over the last 24 months. About 98% of these respondents have indicated that they are knowledgeable of fraud incidents, 69% of which indicated that they had high-level insights up to extensive knowledge of economic crime and fraud incidents in their organizations.

About 45% of the participating respondents are mostly from C-suite and more than 26% are managers and/or head of department. Based on the respondents' primary role in the organization, 30% occupy the executive management board level, 22% are auditors, and 14% are working in the finance department.

Respondents' job title/role

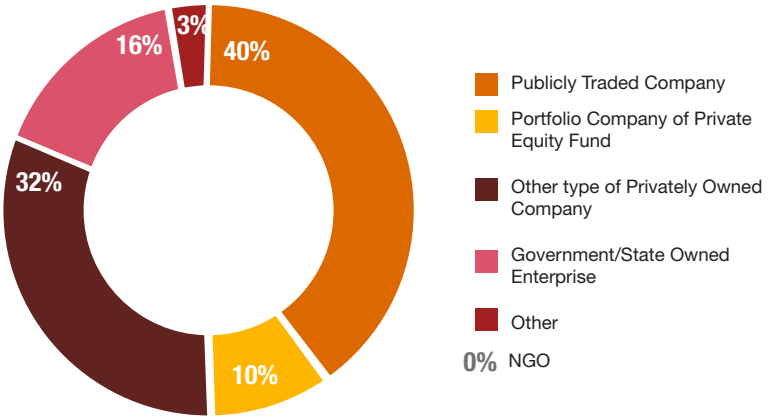


In terms of corporate ownership structure, more than half of survey respondents operate within the country – 14% of which are Filipino-owned domestic corporations. Approximately 40% of respondents are publicly traded companies, 32% are other types of privately owned companies, 16% are Philippine Government-owned enterprises, and 10% are portfolio companies of private equity funds.

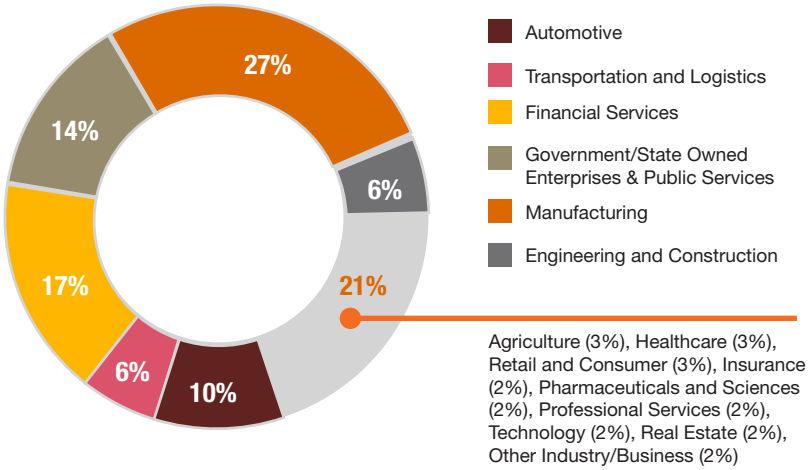
A majority of the subject respondents belong to the manufacturing sector (27%), financial services (17%), government-owned and controlled corporations (14%), automotive (10%), and other various industries (32%). The above respondents from financial services are 100% engaged in banking & capital markets.

Further analysis of respondents revealed that about 22% belong to small-scale businesses with up to 500 employees, 48% belong to medium-size organizations having 501 to 10,000 employees, and 27% work in an organization with more than 10,000 employees in all its operations globally. Annual turnover of these businesses ranges from US$10m up to US$10bn or more.

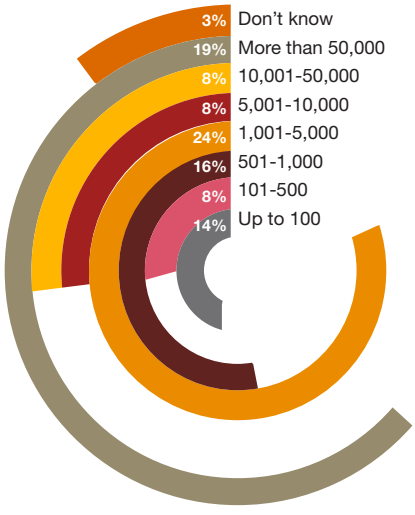
Organizations' ownership structure

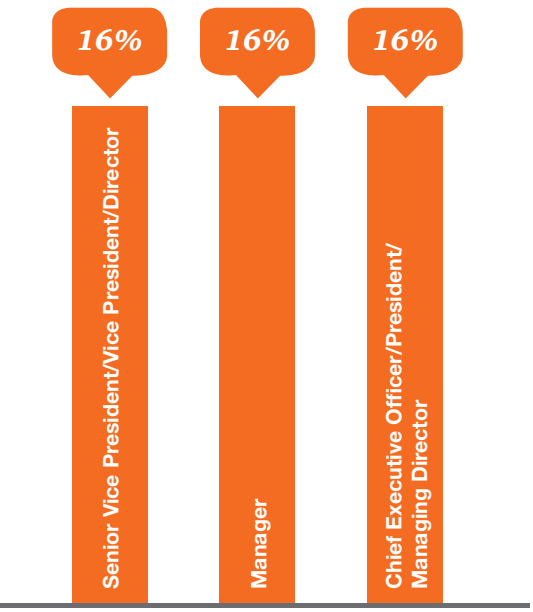


Industries where organizations mainly operate



Number of employees globally





The finer perspective of economic crime in the Philippines

Economic crime and fraud are an obstinate threat affecting both developed and emerging markets. It is important to know how and where perpetrators work as well as the type of scheme that they commit to execute their deceitful plans.

Fraud and economic crime at work

The 2018 GECS results yielded a majority of respondents having experienced various types economic crime[1] and fraud in the work environment. Over the last 24 months, 54% of Philippine respondents (versus 20% in 2016) have indicated that they have experienced economic crime and fraud as perpetrated by internal and external actors. This is quite higher than the global result of 49%.

On the contrary, 41% of respondents have indicated that they have not experienced any economic crime or fraud in their respective local operations while 5% of respondents have said that they do not know if their organizations have had an incident or none at all.

The Philippines' data results are quite higher than global results where 49% of the respondents indicate that they have experienced fraud and 43% mention that they have not experienced any type of incident over the past 24 months.

Back in 2016, one out of three businesses had predicted that they were likely to be affected by economic crime and fraud. Furthermore, 41% of respondents confidently predicted that they were unlikely to be affected by such economic crime over the next 24 months.

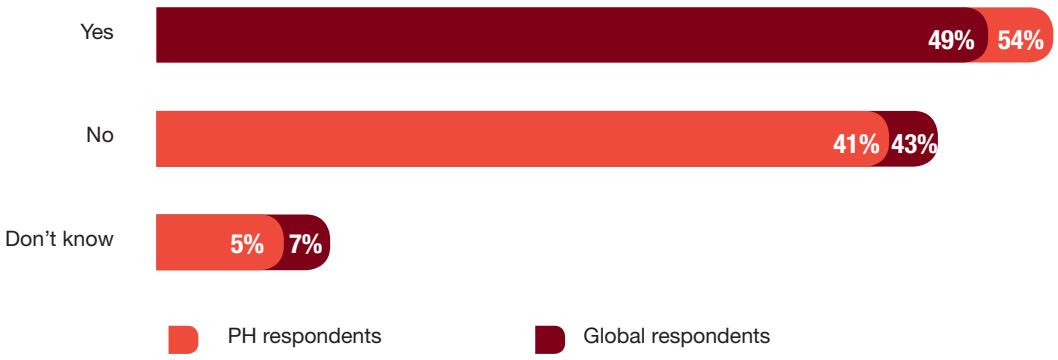
Not until the 2018 results did the footprint of economic crime and fraud in the workplace become visible and the impact of which affected employee morale in the business organization. 48% of respondents have indicated that economic crime and fraud have high and medium impact in the employees' morale, followed by reputation/ brand strength at 27%, business relations at 27%, and relations with regulators at 18%.

In terms of cost spent on investigation of economic crime and fraud incidents, our study revealed that two out of three respondents had spent less on investigation and/or other interventions than the actual amount that the organizations have lost through the economic crime they had experienced.

Furthermore, about 6% of the respondents have mentioned that they have spent the same amount of money for investigation and what have been lost in the incident, while 9% have said that they have spent approximately twice as much as what have been lost in the incident. Lastly, 15% of respondents have not been able to quantify the amount spent by their organizations for investigation and prevention activities.

The financial impact of economic crime and fraud may have a one-time hit of the company's bottomline, but the operational aspect that includes employee morale, reputational/ brand strength, business relations, and relations with regulators, are affected in the long run.

This year's economic crime and fraud in the workplace is quite visible.



1 Economic Crime is the intentional use of deceit or other criminal conduct to deprive another of money, property or a legal right or to effectuate an economic harm. This crime include but not limited to Accounting Fraud, Asset Misappropriation, Bribery and Corruption, Business Conduct/Misconduct (e.g. incentive abuse), Competition/ Anti-Trust Infringement, Cybercrime, Fraud Committed by the Consumer (e.g. mortgage fraud, credit card fraud, claims fraud, check fraud), Human Resources Fraud (recruiting and/or payroll fraud), Insider Trading, Intellectual Property (IP) Infringement, Money Laundering, Procurement Fraud and Tax Fraud.

Top five types of economic crime and fraud in the Philippines

Respondents have been asked on the types of fraud and/or economic crime that their organizations have experienced within the last 24 months. Asset Misappropriation (53%) is still the most experienced fraud incident in the Philippines (same with 2016 GECS results) where one out of two respondents have experienced it. This data is higher by 8%, compared to 45% of respondents who have experienced this type of economic crime globally over the last 24 months.

The second most experienced fraud scheme is Business Conduct/Misconduct (38%), which pertains to frauds or deception by companies upon the market or general public. It comprises deceptive practices associated with the manufacturing, sales, marketing, or delivery of a company's products or services to its clients, consumers, or the general public (e.g. incentive abuse).

The third and fourth most experienced types of fraud incident in the workplace are Procurement Fraud (35%) and Accounting Fraud (29%), respectively. These types of economic crime have always been in the top five of the most experienced fraud incidents in our 2016 study.

The fifth most experienced types of fraud in workplace are Bribery and Corruption (24%) and Fraud Committed by Consumer (24%) where respondents have indicated they have experienced both types of economic crimes over the last 24 months.

Although coming in fifth, Bribery and Corruption remain a serious issue in conducting business in the Philippines. Over the last 24 months, approximately 18% of survey respondents have mentioned that they have been asked to pay bribe and 12% of them have lost an opportunity to a competitor whom they believe have paid a bribe. Back in 2016, 25% of respondents have been asked to pay bribe and 17% have lost an opportunity to a competitor who paid a bribe.

Based on the 2017 Corruption Perception Index by Transparency International, the Philippines ranked 111 out of 180 with a territory score[2] of 34 out of 100.

The Philippines has been consistently rated at 34+ base rate on the annual corruption perception index over the last five years. This indicates that businesses operating in the Philippines have consistently perceived the government as having not implemented any serious mechanism to improve fiscal governance to thwart graft and corruption in the government sector and to protect businesses against this type of economic crime.

Fraud Committed by the Consumer or 'Consumer Fraud', on the other hand, relates to the fraud against a company through illegitimate use of, or deceptive practices associated with, its products or services by customers or others. Examples of this type of fraud include mortgage fraud and credit card fraud.

As it was with the 2016 GECS results, Asset Misappropriation was still the most experienced fraud incident in the Philippines, according to the 2018 GECS Philippine results. 53% of respondents experienced it over the last 24 months.

2 A country or territory score indicates the perceived level of public sector corruption. Transparency International ranks each territory from a scale of 0 – 100 where '0' is considered highly corrupt while '100' is very clean. For the detailed summary, please refer to https://www.transparency.org/news/feature/corruption_perceptions_index_2017#table

The most disruptive economic crime in the Philippines

Unlike their regional and global counterparts, Philippine respondents reported that fraud committed by consumer or Consumer Fraud is the most disruptive of all types of economic crime despite coming in as the fifth most experienced type of economic crime in the workplace over the last 24 months.

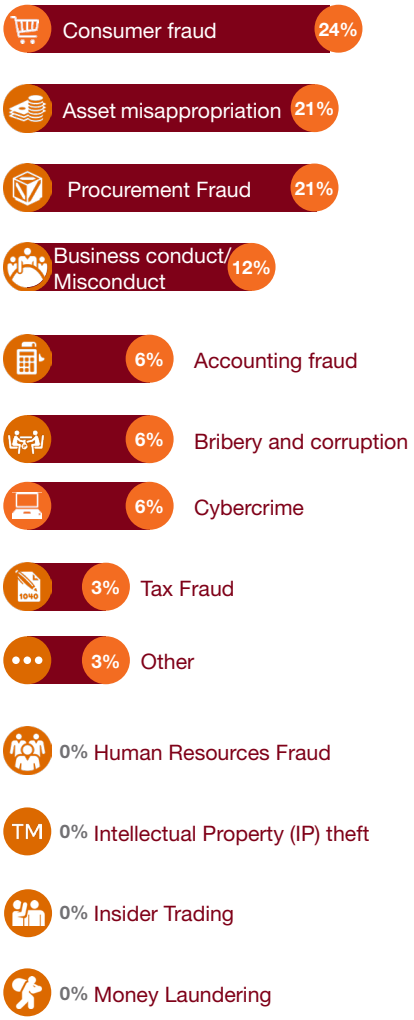
One out of four respondents who had experienced economic crime and fraud in their organization indicated that the consumer related fraud or consumer fraud was the most disruptive in terms of its total impact in the organization (monetary or otherwise). This would mean that organizations were caught off-guard about this type of anomaly and should be more vigilant about it in the future.

Furthermore, one out of five respondents indicated that asset misappropriation (21%) and procurement fraud (21%) are tied as the second most disruptive cases of fraud that they had experienced over the last 24 months.

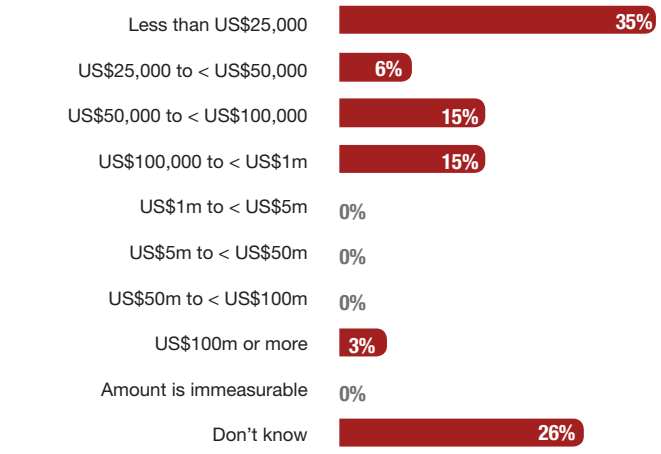
The third most disruptive economic crime was business conduct/misconduct (12%), followed by accounting fraud (6%), and bribery and corruption (6%).

These types of disruptive incidents were brought to the attention of Senior Management or Board Level Executives charged with corporate governance. Because of the most disruptive crimes that happened over the last 24 months, businesses had lost approximately US$25,000 to US$100m, or even more, due to consumer related fraud.

Disruptive economic crimes in the Philippines



Direct loss incurred due to disruptive crime



Emerging threats in the next 24 months

While thinking about the next 24 months, respondents were asked to identify the type of economic crime and fraud that would 'likely' to be the most disruptive/serious incident in terms of its impact on the organization (either monetary or otherwise). The response was quite similar to the current scenario of incidents experienced in the last 24 months. Our study revealed the top five most disruptive economic crimes over the next 24 months: 1) Bribery and Corruption at 16%, 2) Asset Misappropriation at 14%, 3) Procurement Fraud at 13%, 4) Business Conduct/ Misconduct at 11% and Fraud Committed by the Consumer, also at 11%, and 5) Accounting Fraud at 10%.

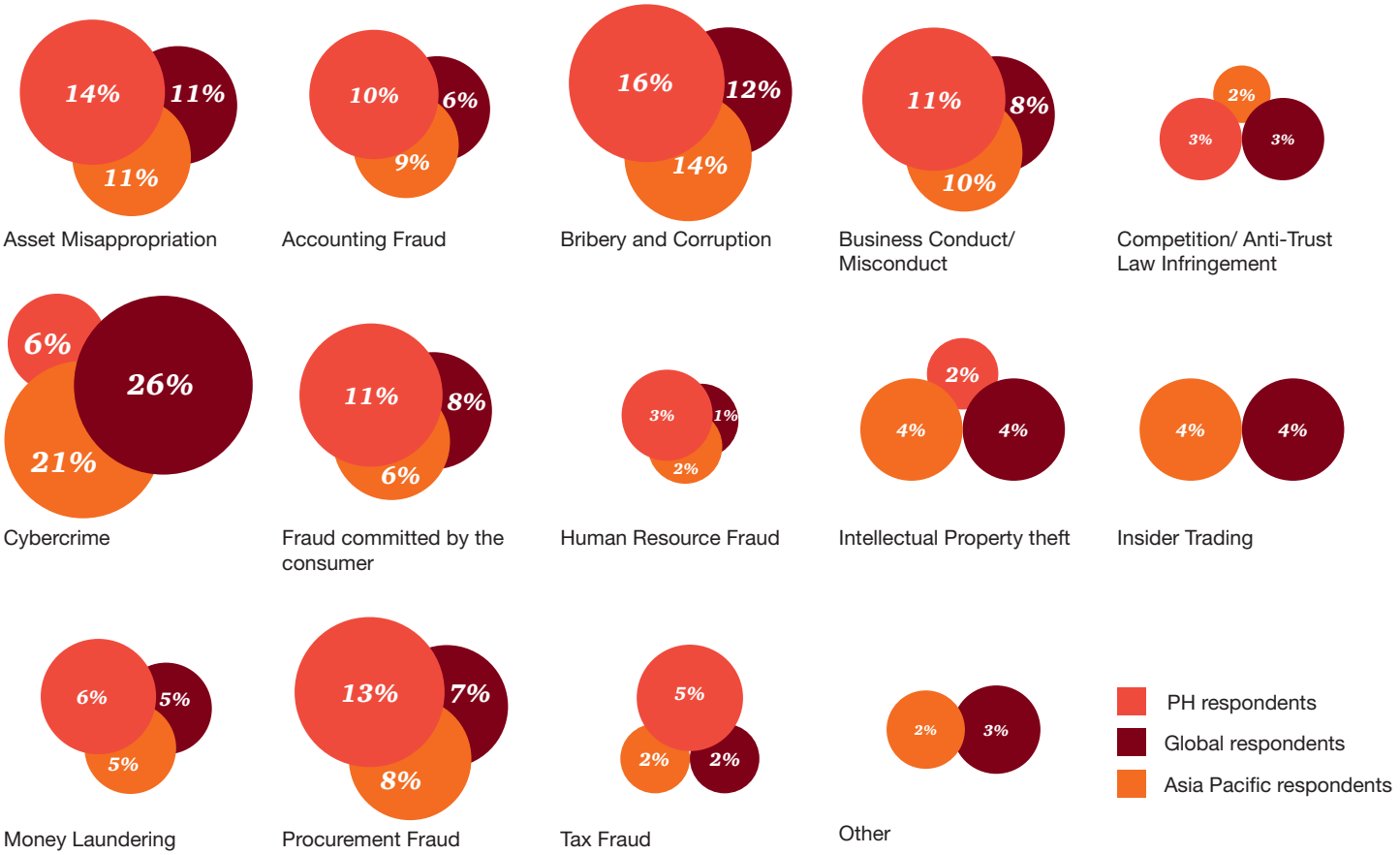
Our survey showed that bribery and corruption were still perceived as one of the top five economic crimes in the country that would hit the headlines over the next 24 months.

Unless the current administration changes its fiscal governance to fight bribery and corruption to support the business sector in growing the economy over the next 24 months, the stigma of the Philippines being seen as a corrupt country within the Asia Pacific region will still go on despite its potential market growth in the ASEAN region.

Economic crime and fraud – a lurking business risk

Our study of economic crime and fraud for 2018 is an eye-opener for businesses in the Philippines: economic crime and fraud should be considered as part of the overall operating business risk that must be managed accordingly at the Executive/ Board level. On a positive note, the majority of respondents are conducting general risk assessment, cyberattack vulnerability tests, and anti-bribery and corruption assessments.

Most disruptive economic crimes over the next 24 months



However, one out of five or approximately 20% of respondents admitted that they have not performed any risk assessment in their organization in the last 24 months. Absence of any risk assessment on the enterprise level exposes any business to economic crime and fraud risks that may eventually cause unnecessary losses.

It is interesting to note, however, that in 2016, businesses predicted that the top five economic crimes over the next 24 months would be: 1) asset misappropriation, 2) bribery and corruption, 3) cybercrime, 4) procurement fraud, and 5) human resources fraud.

But the 2018 results have instead revealed different types of economic crime and fraud: 1) asset misappropriation, 2) business conduct/ misconduct, 3) procurement fraud, 4) accounting fraud, and 5) bribery & corruption and consumer fraud.

Consequently, cybercrime and human resources fraud landed as the seventh and sixth most experienced economic crime and fraud in the Philippine workplace over the last 24 months.

A lurking enemy within

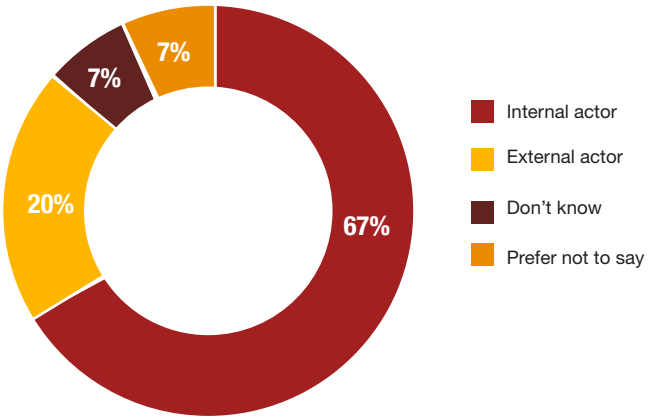
As earlier mentioned in this report, 54% of Philippine respondents admitted that they had experienced economic crime and fraud over the last 24 months. Such anomalous schemes could have been perpetrated by either an internal or external actor or a combination of both. The magnitude of financial impact of such a crime may be determined by the type of incident encountered by the concerned organization.

But when the above respondents who experienced fraud were asked *"Who was the main perpetrator of fraud?"*, a majority of them (53%) intentionally "skipped" this section of the survey. For whatever reason that they may have, only 47% of respondents shared critical information (for case study purposes) about the details of economic crime and fraud that they had experienced over the last 24 months.

With the foregoing fact, it depicts how Philippine businesses (who had experienced economic crime and fraud) are "not too open to share more information" – publicly. Though the survey results are totally confidential, concerned respondents have opted to skip this part of the survey to protect their organizations from unnecessary exposure to regulators and/or the general public.

Top economic crimes in the Philippines

Main perpetrators of fraud



Current selection: Philippines

Consequently, the indicative data[3] from participating respondents have revealed that at least two out of three fraud incidents were perpetrated by internal actors, e.g. senior management, middle management, junior management, and other staff members.

Our study yielded an interesting fact that among the territories covered in the global survey, the topmost internal actors who committed economic crime and fraud include middle management (37%), junior management (26%), senior management (24%), and other staff (11%).

The indicative results in the Philippines are comparable with the global results where internal actors mostly belong to the principal functions of executive management, operations and production, marketing and sales finance, procurement and customer service.

On average globally, the principal function of internal actors resides in almost all key departments having fiduciary responsibilities over the daily operations of the company. Whatever fiduciary capacity that was delegated to the internal actors, plus weaknesses in management control systems (for failure of internal controls), equate to an excellent opportunity to commit and perpetrate white-collar crime without being detected. Such excellent opportunity is capitalized by internal actors because "they can" manipulate and circumvent existing management control systems and get away with their crime.

Our survey results are similar to the results of the study made by the Association of Certified Fraud Examiners (ACFE) where business owners/ executives accounted for a small percentage of fraud cases globally. However, it caused huge median losses that hit the company's bottomline.

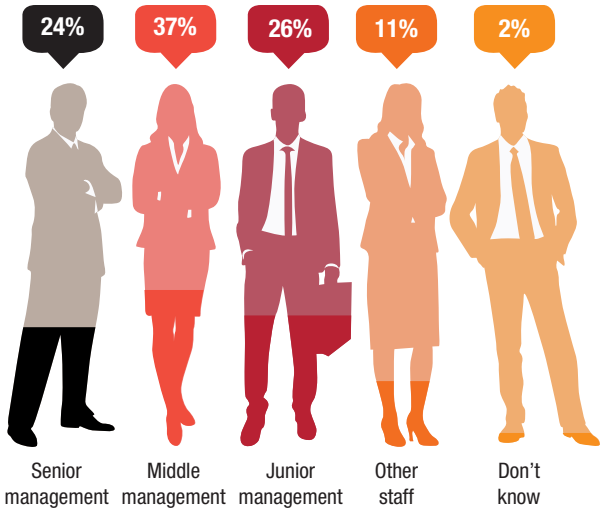
On the other side of the fence, another actor is lurking around, waiting for the perfect timing to unleash his destructive scheme within the organization. Our study revealed one out of five or 20% of the economic crime incidents have been perpetrated by external actors.

The external actors include, but are not limited to, vendors, customers, agents/intermediaries, organized crime, competitors, hackers, third-party contractors, consultants/advisors, customers, and other stakeholders who know the vulnerabilities of the organization's internal controls and/or collaborate with (an) internal actor(s).

In the global environment, the top five external fraud perpetrators are customers (39%), cybercriminals/hackers (31%), organized crime (22%), agents/intermediaries (16%), and vendors (13%).

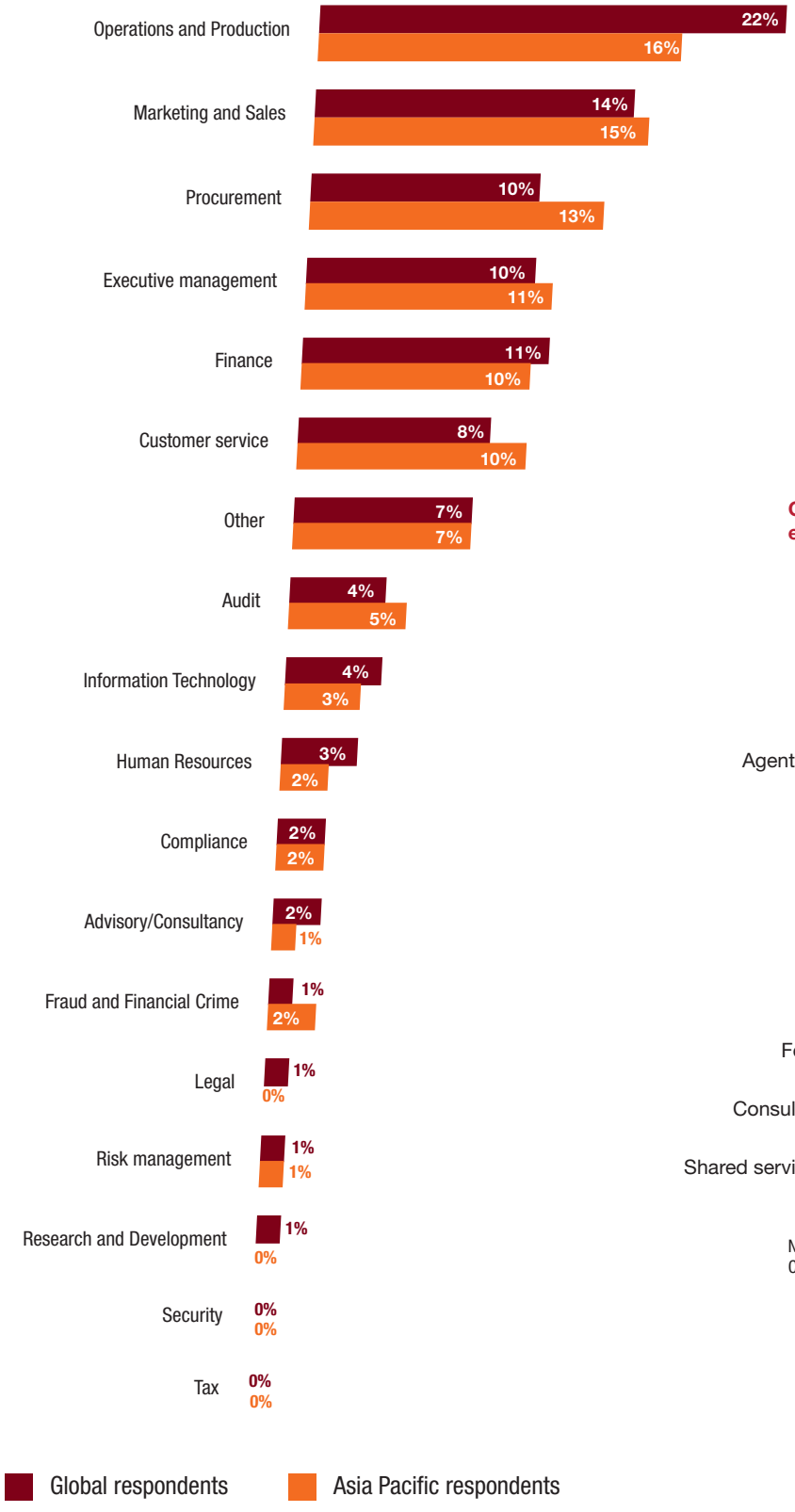
According to the ACFE's Report to the Nations , the median losses brought about by occupational fraud in the organization are far greater when a perpetrator colludes with other fraudsters.

Main perpetrators of internal fraud (global data)

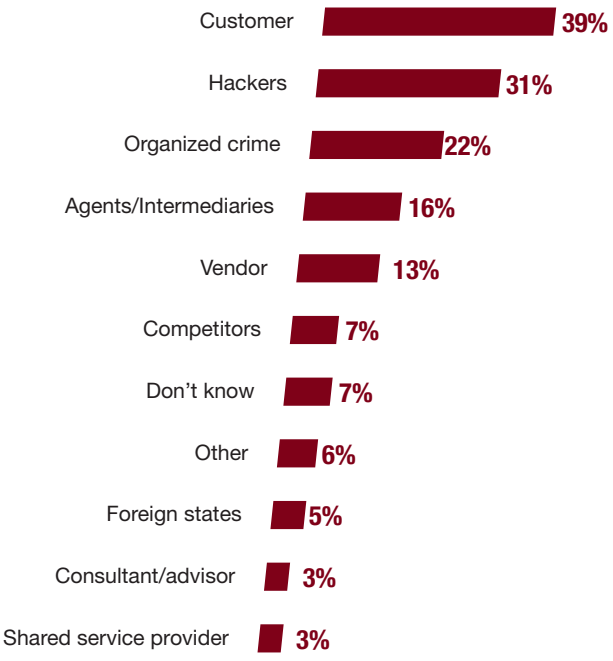


3 PwC cannot draw conclusions on the data results for the question: *"Who were the main perpetrators of that external fraud against your organization?"* due to low base of respondents who attributed the fraud incidents either from internal or external actors.

Q: Which principal function did the MAIN perpetrator of the internal fraud reside in?



Q: Who were the main perpetrators of that external fraud against your organization?



Note: Respondents were asked to select all that apply
Current selection: Global

Cybercrime on the rise

Cyberthreats climb up year after year, thus, this is a call for preparation and greater leadership involvement. Cyber preparedness should be seen as an organizational stress test.

As Philippine businesses harness their growth potential in the region, and with the country considered as having the fastest-growing economy[4] in ASEAN, their dependencies on technology are becoming increasingly vital to support that development and expansion beyond boundaries. At this juncture, Philippine businesses are not spared from cyberattacks.

Our study reveals that in the last 24 months, over a third of Philippine respondents have been targeted by cyberattacks. These incidents have been perpetrated by both phishing (27%) and malware (32%) attacks. A similar trend was observed in the Asia Pacific region (29% and 33%) and global respondents (33% and 36%), respectively.

Most of the cybercrimes reported globally had caused business disruption and exposed personally identifiable information (PII), which continues to be the prime target of cybercriminals. It would only cost US$50 for cybercriminals to steal PIIs for reselling several times in the black market.

Q: In the last 24 months, has your organization been targeted by cyberattacks using any of the following techniques?

	Results
Network scanning	8%
Brute force attack	2%
Phishing	27%
Man in the middle	5%
Malware	32%
Other technique	3%
Yes but do not know the specific technique	5%
No	32%
Don't know	21%

Governance and cybersecurity program

With cyberattacks becoming prevalent in all business sectors globally, more and more companies are investing in governance and technical aspects of information security. Awareness trainings on cyberthreats and its disruptive effects to the organizations should be communicated to employees to prepare them for an eventual cyberattack.

About 59% of surveyed organizations have fully operationalized their firmwide cybersecurity program

In 2016, one in every three organizations had either a fully operating cybersecurity program or had such a plan but not fully implemented across the organization. Since then, Philippine businesses had embraced the importance of having existing operational cybersecurity programs implemented to protect their information assets.

Our study indicated that about 59% of respondents have developed a fully operational cybersecurity program. This increased focus on cybersecurity is likely a result of regulatory pressure to comply with the Data Privacy Act of 2012 ("DPA" or R.A. 10173). The DPA requires organizations to implement organizational, physical and technical safeguards to ensure that personal data processing is done in a transparent, legitimate, proportional manner which preserves the data privacy rights of individuals. These safeguards intersect with cybersecurity controls and has contributed positively to the improved cybersecurity posture of Philippine organizations.

To make this cybersecurity program more beneficial to the organization, and to comply with regulatory requirements, senior leaders are prompted to take the lead and be in charge of the overall cybersecurity and resilience checks for the organization. Board members are expected to be more engaged as part of their corporate governance responsibilities. One third (1/3) of respondents have indicated that their respective organizations have designated a Chief Information Security Officer (CISO) and most of these CISOs directly report to the board-level executives.

4 de Vera, Ben O. (2018, January 10), *Philippine Daily Inquirer*. PH to remain fastest-growing economy in ASEAN — World Bank. Retrieved from http://business.inquirer.net/243868/breaking-business-world-bank-asean-economy-fastest-growth-2018-global-economic-prospects-gdp

38% of respondents were optimistic and were open to adopt the Global Beneficial Ownership standards, as they believed it will be beneficial for organizations in combating economic crimes and frauds

One out of every two, or nearly half of respondents, have mentioned that the cybersecurity program in their organizations contains specific cybersecurity policies. One of the key components to be added in information security programs is the development of an incident and breach response plan for cybercrimes that include, among others:

- procedure for the timely discovery of security incidents
- clear reporting lines in the event of a possible breach
- an evaluation of the security incident or immediate and long-term damage
- the impact of the breach
- policies and procedures for mitigating possible harm and negative consequences of the cybercrime.

Cybersecurity awareness – a serious business issue

Only 9% of Philippine respondents claim to have been victims of cybercrime compared to 17% in the 2016 GECS report. In contrast, one-third of global respondents have reported encountering cybercrimes in 2018.

Lack of awareness about the type of fraud and cybercrime can be a reason for the drop in crime rate. This is clearly reflected in our survey where 53% of respondents (who reported encountering cybercrime) are not aware of techniques used by external hackers to execute a cyberattack.

In order to combat cybercrime, the first step is to be aware of the types of cybercrime to help identify red flags within an organization, and to have a holistic approach to manage the organization's vulnerability against cyberthreat agents. It is essential to provide employees and representatives with periodic training sessions as a first line of defense so that: 1) all internal stakeholders are aware of the types of cyberthreats, and 2) they are prepared to respond in case they face any cyberthreat. Our study indicates that about 43% of respondents have reported that their organization's cybersecurity programs include awareness training for employees, especially for cybersecurity personnel.

Technology adoption

The use of technology in combating economic crime and fraud helps organizations attain resilience on cyberthreats by enabling real-time monitoring; providing actionable insights; integrating and managing workflow or processes; and enabling identification, remediation and documentation of dispositions of cyberthreats.

Most of the organizations in the Philippines are using technology as a tool to monitor cyberattacks (similar to global and Asia Pacific companies) and detect fraud, followed by business conduct. Global and Asia Pacific organizations also use technology for third-party due diligence reviews, sanction screening, and anti-bribery/anti-corruption activities. Alternative/disruptive technologies and techniques are used for

Q: To what degree is your organization leveraging Artificial Intelligence or Advanced Analytics to combat/monitor for fraud and other economic crimes?

	Using and finding value	Using but not finding value	Plan to implement in the next 12 months	Under consideration	No plans to use	Don't know
Machine Learning	5%	0%	2%	8%	31%	54%
Natural Language Processing (NLP)	0%	0%	2%	8%	32%	58%
Natural Language Generation (NLG)	0%	0%	2%	8%	32%	58%
Voice Recognition	2%	0%	3%	7%	32%	56%
Predictive Analytics	2%	0%	3%	8%	29%	58%

45% of surveyed organizations in the Philippines are using technical elements in cybersecurity for network monitoring

email monitoring, transaction testing, monitoring, creating dashboards, periodic analysis, and anomaly detection.

Furthermore, our study reveals that a majority of the organizations are using technology as tool for network-monitoring appliances (45%) to monitor cyberattacks, fraud detections, and application security practices; followed by business conduct and breach notification protocol (40%). Less than a third of respondents mentioned about penetration testing and vulnerability assessments, which need more attention as these ensure safety and security of an organization's IT infrastructure. Global and Asia Pacific organizations also use technology for third-party due diligence, sanction screening and anti-bribery/anti-corruption, which is not very significantly reported by business organizations.

Impact of geopolitical environment

Companies in the Philippines are optimistic about their readiness to face economic crimes over the next 24 months. About 37% of respondents expect an increase in their appetite to spend on resources to fight against economic crimes and fraud, which is higher than the data in other territories, as well as globally and in the Asia Pacific region.

However, when it comes to impact of geopolitical environment on opportunities to commit economic crimes and fraud, the companies in Philippines (as well as global and Asia Pacific) are less optimistic. About 25% of respondents expect an increase and another 25% suggest that geopolitical environment will not have an impact.

37% of respondents expect an increase in their appetite to spend on resources to fight against economic crimes/fraud

More than 50% of respondents feel that the recent changes in geopolitical environment will lead to changes in regulatory environment and enforcement of regulation in their organization. This was observed across global and Asia Pacific respondents.

Business imperatives necessary to combat economic crime and fraud

Internal or external actors who commit fraud in organizations and who continue to achieve their schemes successfully stem from the organizations' lack of preparedness. These organizations should be a step ahead of potential fraudsters and embark on investing in people and technology.

Robust management control systems

It is fundamental for businesses to secure their assets. To do this, an organization must have robust management control systems. These are internal controls at the enterprise level down to the sub-department and sections where the company operates. Based on our study, the combination of these two is the most effective way to detect economic crime and fraud.

Setting up appropriate corporate controls

A risk-based internal audit function plays a vital role in preserving the integrity of corporate controls across the organization. With an independent function and authority from the Board of Directors, they make use of data analytics tools as well as a system of continuously monitoring suspicious activity – a formidable combination of technical know-how to effectively detect anomalies and red flags in the organization.

Building and maintaining an ethical corporate culture

An enhanced corporate culture is also an effective defense in combating fraud. About 20% of respondents indicated that fraud in their organizations were reported through an internal tip-off or through an internal fraud reporting system, and 10% said it was through a tip-off from external parties. A whistleblowing hotline/ portal may serve the purpose of receiving internal tips. Employees are encouraged to report any form of anomaly to management without any fear of retaliation from any source.

About 80% of the respondents have indicated that they have a formal business ethics and compliance program in their organization. These organizations have pre-defined specific policies and tailored controls over:

- general fraud
- anti-bribery and corruption
- sanctions and export controls
- anti-money laundering
- anti-competitive/anti-trust
- cyber behavior
- industry-specific regulatory compliance.

Specific policies should be consistently applied across organization. To ensure that the business ethics program is effective, organizations may conduct the following:

- periodic internal reviews
- management reporting
- monitoring whistleblowing hotline reports
- review by third party consultants.

Our survey reveal that 85% of respondents have been conducting periodic internal reviews in workplace. The Chief Compliance Officer has the primary responsibility over the full and consistent implementation of business ethics and compliance program within the organization.

Effective risk and vulnerability assessments

Over the last 24 months, one out of two businesses in the Philippines has been conducting general fraud risk assessment in their organizations to proactively manage fraud risks. These businesses are aligned with the general fraud risk appetite of its counterparts in the Asia Pacific and the global organizations.

Our study reported that risk assessment was designed as part of (a company's) annual routine process – 65% of the respondents have indicated that it is part of the audit plan and 35% have indicated that it is part of Enterprise Risk Management (ERM) strategy.

Respondents have also reported that their risk assessments have been designed as part of its annual routine process – 65% of the respondents have indicated that it is part of the audit plan, and 35% indicated that it is part of Enterprise Risk Management (ERM) strategy.

There are also a few business organizations whose risk assessment strategies have been driven by specific event. However, it is quite a surprise to know that even at this time, 19% or approximately one out of five organizations has not done any type of risk assessment over the past 24 months. This leaves them vulnerable to all business risks that organizations may encounter over the next two years.

Types of risk assessments conducted in organizations over the last 24 months

Aside from general fraud risk assessment that came out on top of the list at 51%, respondents confirmed that they assess their organization's exposure to bribery and corruption (29%) and their vulnerability to cyberattacks (29%).

For anti-money laundering exposures, however, only 19% of the respondents have performed risk assessment on such. These respondents, who are mostly from the Financial Services sector, are required by local regulations to adhere to Republic Act No. 9160, also known as the "Anti-Money Laundering Act of 2001". Non-financial services respondents have not done any anti-money laundering assessments in their organizations since they are not required by government regulators. These sectors include manufacturing, government-owned enterprises, automotive, engineering & construction, and transportation & logistics.

Investing on people and anti-fraud tools

Depending on the fraud risk appetite, many organizations have invested in technology as a vital tool to combat fraud in the workplace. But this is only part of the solution to protect company assets.

Most businesses have decided to initiate investing not only in technology but in its people as well.

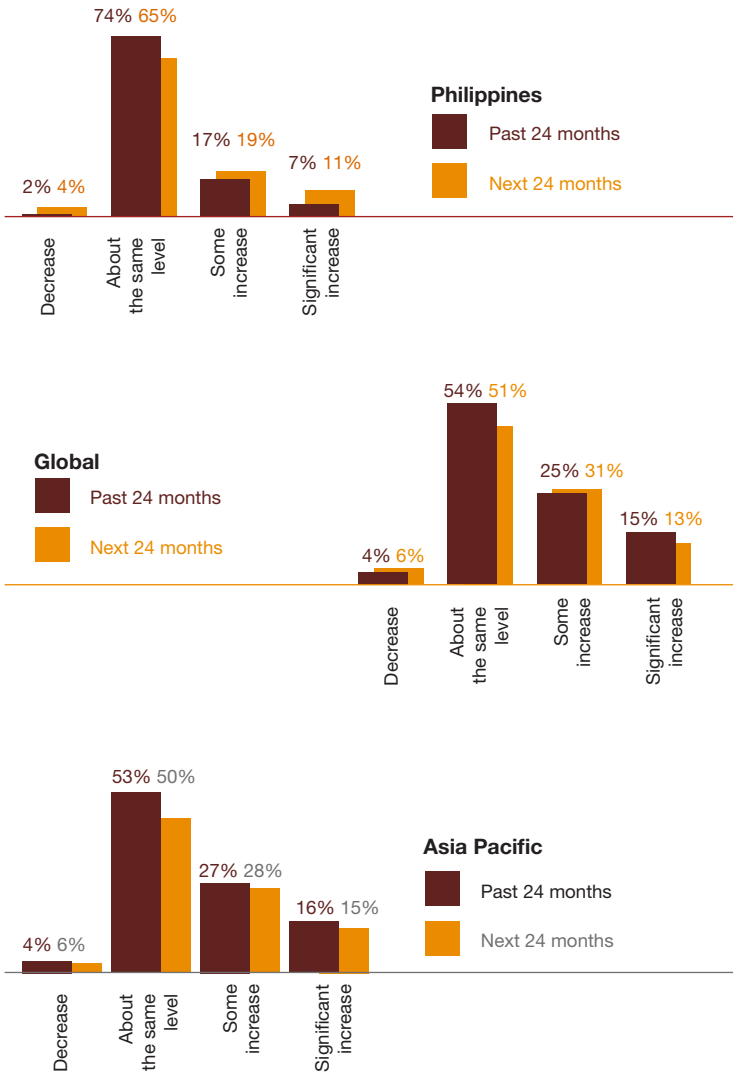
Over the past 24 months, three out of four respondents have indicated that their organizations will spend the same amount of investment in combating economic crime and fraud. The same number of respondents have mentioned that they will spend the same amount of investment over the next 24 months. Only 11% of the respondents have indicated that they will increase their investment significantly over the next two years.

Anti-fraud tools include:

- conducting an enterprise-wide fraud risk management and vulnerability assessment regularly
- developing a whistleblowing framework that includes maintaining a hotline or portal where employees are encouraged to report any anomaly that they know and/or uncover within the organization
- investing in anti-fraud training to equip employees on the latest trends on fraud
- investing in automated tools and data analytics techniques to continuously monitor unusual data transactions.

Risk assessment performed by organization

Amount of funds used to combat fraud



Contacts

Roberto C. Bassig
Partner
roberto.c.bassig@ph.pwc.com
T: +63 (2) 845 2728 local 3143

Aurelio Mari G. Gueco, CFE
Senior Manager and Forensics Leader
aurelio.mari.gueco@ph.pwc.com
T: +63 (2) 845 2728 local 3231

www.pwc.com/ph