Economic uncertainty

Unethical conduct

How should over-burdened compliance functions respond?

Asia-Pacific Fraud Survey 2017

The better the question. The better the answer.
The better the world works.

EY
Building a better working world

Contents

Introduction

In a year characterized by geopolitical risk, economic uncertainty and increased regulatory intensity, the findings of our 2017 Asia-Pacific Fraud Survey are cause for concern. Our survey highlights multiple 'red flags' indicating that organizations are in danger of letting fraud risk spiral out of control.

The findings reveal that current compliance programs in the region are not yet resulting in ethical employee behavior. Despite increased organizational efforts to combat fraud, bribery and corruption, significant numbers of the almost 1,700 employees surveyed believe a wide range of unethical behaviors are justified to help a business survive. At issue is a perceived lack of ethical leadership. Compliance policies may be in place but, under pressure to deliver growth, some senior managers are ignoring unethical actions to achieve corporate targets.

As a result, the more than 90% of employees who said they want to work for a company with a strong compliance culture are in a difficult situation. The vast majority said they want to do the right thing, but compliance policies are neither clear nor consistently applied. Our 2017 survey finds that a significant minority of employees are aware of, but have not reported, fraudulent activities.

Part of the issue is that a worrying number of employees don't trust their organizations. Substantially more employees would rather report wrongdoing through an external channel, such as the police or a government authority, than use an internal whistleblowing hotline.

Over the last few years, many companies have failed to fill all the roles required to operate a robust compliance framework. With anti-bribery and anti-corruption (ABAC) policies failing to improve ethical conduct and regulatory enforcement in the Asia-Pacific (APAC) region at an all-time high, the reduced budget, and the slowing recruitment that economic uncertainty may cause, could create a dilemma for compliance teams.

Our survey suggests that organizations in APAC need to rethink their approach to compliance. Employees need absolute clarity around what policies mean and what compliant behavior looks like.

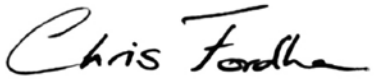
Leadership must:

- Incentivize ethical conduct
- Encourage, protect and reward whistleblowers
- Take transparent and consistent action against misconduct

To detect unethical behavior with fewer resources, companies need to harness technology including, forensic data analytics.

We hope the following results and analysis give executives and boards a valuable new perspective on the ethical leadership needed to manage fraud, bribery and corruption risks effectively and efficiently in the uncertain times ahead.

We also acknowledge and thank all of the respondents for their contributions.



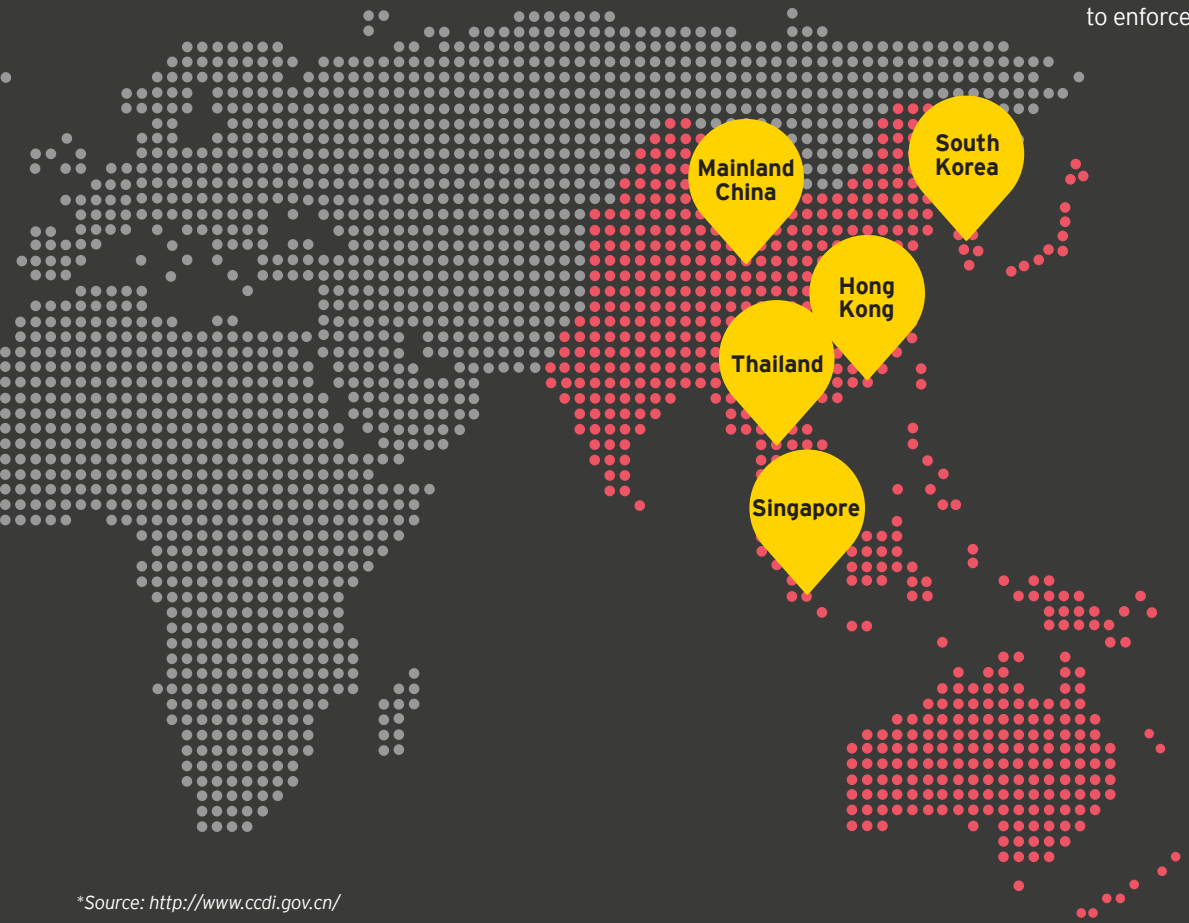
Chris Fordham
EY Asia-Pacific Leader
Forensic & Integrity Services

Executive summary

Our 2017 survey finds considerable evidence of increasing fraud risk. Significant numbers of respondents do not know about or do not understand compliance policies. A third do not feel comfortable reporting unethical behavior. Many are unaware of key fraud, bribery and corruption risk areas. As a result, as many as two-thirds of APAC employees said they are taking actions that they know are unethical or risky. A quarter say their colleagues are failing to report misconduct. Against a backdrop of economic and geo-political uncertainty, organizations need strong ethical leadership to give employees a better moral compass when making day-to-day workplace decisions.

Since our 2015 survey, the region's regulators have increased their targeting of, and tightened their penalties for fraudulent behavior. In 2016:

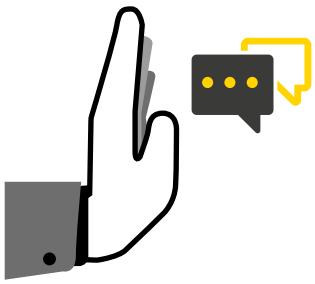
- **Mainland China** updated the monetary thresholds for bribery prosecutions and sentencing, and extended the scope of bribes to include intangible benefits. The Central Commission for Discipline Inspection* issued over 450,000 disciplinary penalties and 11,000 people were investigated by judicial authorities.
- **Singapore**'s Monetary Authority set up a dedicated team to monitor anti-money laundering (AML) risks and carry out onsite supervision of how financial institutions manage these risks.
- **Thailand** strengthened its anti-corruption laws to help curtail bribery and collusion.
- **South Korea** enacted the "Improper Solicitation and Graft Act" imposing vicarious liability on companies where employees or agents commit offenses unless the company exerted due care and supervision to prevent such conduct from occurring.
- **Hong Kong**'s Securities and Futures Commission set up specialized teams to pursue corporate fraud and AML as a priority, as part of its shift toward a more targeted approach to enforcement.

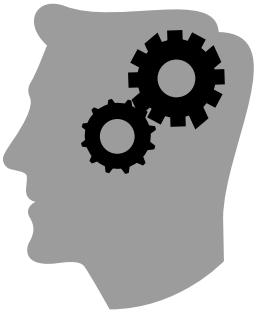


Source: http://www.ccdi.gov.cn/

Global cooperation is on the rise, with the work of the G20 (Group of 20) and B20 (Business 20) platforms and others having a noticeable effect. Never before have governments cooperated so extensively in combating bribery and corruption and imposing legal sanctions against fraud. As a further complicating factor, anti-corruption and anti-trust regulations are becoming entwined, increasing the complexity and difficulty of compliance.

In this environment of increasing regulatory pressure and complexity, our 2017 survey finds:





- **Ethical standards are not improving**

  Despite survey respondents reporting that the majority of organizations have expanded or sustained their efforts to combat fraud, bribery and corruption, this investment in compliance policies and processes are not always translating into ethical conduct. More than a third of our respondents report that bribery is commonplace in their industry.

- **Standards are not being applied consistently**

  Almost half of our respondents warn that managers are ignoring unethical behavior and justifying misconduct to meet business targets, resulting in organizations where people do not feel comfortable reporting fraud, bribery and corruption. Distrust in whistleblowing hotlines has reached the point where some employees would rather go direct to the authorities than use an internal communications channel.

- **Compliance lacks clarity**

  Our survey also finds a significant number of employees do not understand critical elements of compliance policies and processes, highlighting areas where organizations need to strengthen their ethical leadership. For example, the findings indicate worrying levels of misunderstanding around ABAC policies and the risks surrounding cyber and insider threats.

Call to action

With an increased number of respondents prepared to start looking for another job if their organization were to become involved in a major corruption scandal, providing strong ethical leadership has never been more critical. To ensure compliance policies deter unethical conduct, APAC business leaders must provide absolute clarity and consistency around how to reduce the risks associated with fraud, bribery and corruption. Companies should:

1. Revisit ABAC policies

Existing ABAC policies should be simplified, made more succinct, provided in the local language and explained in terms of real-world examples. Organizations that don't have them need to introduce clear gift-giving and entertainment policies. To make policies effective, all leaders, including line managers, must proactively educate employees that compliant behavior is not a hindrance to commercial success, and incentivize and empower employees to make compliance a top priority.

2. Harness forensic data analytics

Forensic data analytics (FDA) is key to keeping up with the mountains of data organizations must sift through to prevent and detect fraud, bribery and corruption. Compliance teams need to harness FDA to monitor the full range of data points – not just looking for red flags in financial data, but also proactively using sentiment analysis of emails (where legally permissible), and text to detect early warning signs of misconduct.

3. Raise the bar for third parties

As companies look to grow their businesses in the region's emerging markets, compliance programs will need to raise the bar to include multiple ABAC and anti-competition laws and regulations, especially with APAC regulators continuing to focus on the risks third parties pose to companies.

4. Benchmark whistleblowing hotlines

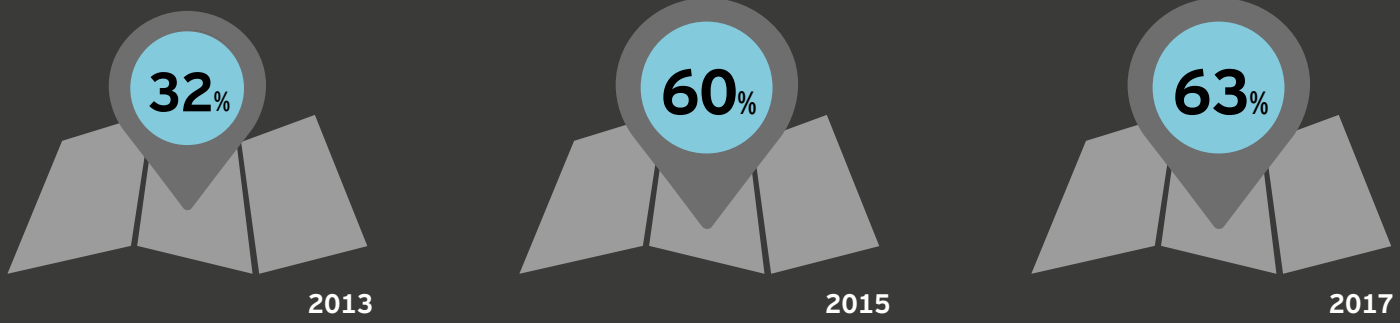
Benchmarking will help organizations to identify how to improve their whistleblower protection and effective reporting mechanisms. APAC companies must adopt and enforce policies to protect whistleblowers from retaliation and ensure appropriate, consistent and transparent follow-up to their disclosures.

5. Treat data risk as one holistic program

Cyber criminals, hackers and malicious insiders are targeting organizations for their sensitive commercial information as well as their cash. Companies are increasingly vulnerable through careless employees and others not following technology security protocols. As a result, cyber and insider threats have become part of one larger data risk that will require a holistic approach for its prevention, detection and investigation.

Bribery or corrupt practices happen widely in my

country



Major factors challenging my business

Slower growth than expected in my country

62%

Political instability in my country

50%

Economic uncertainty of my country

64%

Increased regulation in my sector

59%

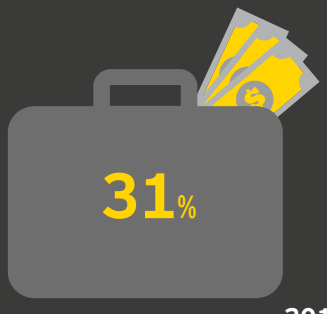
Q. Are any of the following increasing the challenges for the growth or success of your business?

Base: Total respondents (1,638), except government / public sector employees

It is a common practice to use bribery to win contracts in my

industry or sector

2013



2015

2017

Trend confirmed: employees won't work for unethical companies

Two years ago, our 2015 survey uncovered a new dimension to non-compliance. For the first time, the vast majority of respondents, especially Generation Y[1], said they would leave, or refuse to join, companies they knew were involved in fraud, bribery and corruption scandals.

Since then, against the backdrop of increased anti-corruption enforcement and the threat of economic instability, our 2017 survey findings show this attitude has become even more entrenched. More employees than ever say they would vote with their feet if their organization was involved in a major fraud, bribery or corruption scandal. A notable 87% of respondents under the age of 25 and 82% of all respondents said they would start looking for another job (up from 78% in 2015), including 37% of all respondents who would be unwilling to continue working for their company (up from 29% in 2015).

Two-thirds of respondents regard a good reputation for ethical behavior as a commercial advantage. But their desire to work for a compliant company is not just about wanting to be on the "winning team" – it goes to strongly held personal values around integrity, honesty and ethics. When choosing a job, 93% of respondents say compliance culture was an important factor in deciding which company to work for. More than two in five say that they would sacrifice salary to work for an ethical employer.

These findings suggest that organizations with a strong compliance culture will continue to be the big winners in the recruitment and retention of talent.

4 in 5

Generation Y[1] respondents would **look for another job** if their organization was involved in a major fraud, bribery or corruption case

2 in 5

respondents would be **prepared to earn less** in order to work for ethical organizations

[1] *25-34 years old*

93%

of respondents consider **compliance culture to be an important factor while choosing their future workplace**

82%

of respondents say that if an organization was involved in fraud, bribery and corruption, **it would affect their willingness to work for that company**

"The findings prove that compliance attracts talent. People prefer a secure, compliant corporate environment rather than being put in a situation where they feel pressure to behave unethically. There has never been a more important moment for employees to understand, trust and feel empowered by compliance."

Emmanuel Vignal, Greater China Leader, Forensic & Integrity Services

Why aren't ethical standards improving?

In response to increasing pressure from regulators, investment in compliance programs across the region is at an all-time high. Yet ethical standards show few signs of improving.

Our 2017 survey findings show that compliance policies and processes are not translating into ethical conduct, despite increasing numbers of APAC companies putting these compliance elements in place.

More than four in five (83%) respondents report organizational efforts to combat fraud, bribery and corruption have been expanded (51%) or sustained (32%) in the last two years, with an upward trend in the percentage of organizations with ABAC policies and codes of conduct.

After some countries, such as India, introduced legislative requirements for whistleblower provisions, the region has also seen a 6% jump in organizations with whistleblowing hotline programs. Three in five (61%) respondents report that their organizations now have hotlines in place.

Yet, despite this investment in expanding the compliance framework, more than half of our respondents (52%) still feel ethical standards have not improved in their organizations. More than two-thirds (69%) say they have had information or concerns about misconduct in their company. This is higher than findings in the EY Fraud Survey 2017 for Europe, Middle East, India and Africa (EMEIA), where only 52% of respondents expressed similar concerns.

The percentage of respondents who had seen people with questionable ethical standards being promoted rose to 43% – up from 40% in 2015. More than a third (35%) say it is still common to use bribery to win contracts.

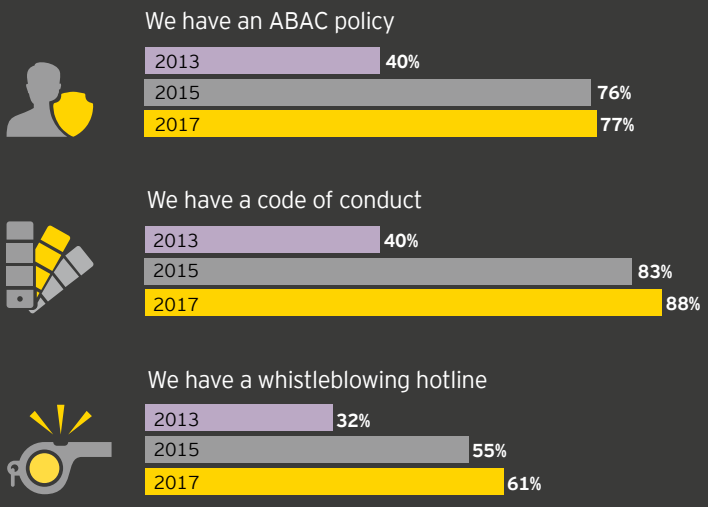
Clearly, more compliance investment isn't translating into more ethical conduct. Our 2017 survey findings suggest that this is because:

1. Standards are not being applied **consistently**
2. Compliance lacks **clarity**

52% of respondents believe that **ethical standards have not improved** in their local business operations

43% of respondents have seen **people with questionable ethical standards being promoted**

Steady growth in compliance policies and processes



> "When organizations promote people with questionable ethical standards, their behavior becomes contagious. These people replicate this practice, which they've rationalized as being acceptable, throughout their new team and misconduct spreads."
>
> **Diana Shin, Partner, Forensic & Integrity Services, China**

Standards are not being applied consistently

Respondents tell us that senior managers are ignoring unethical behavior and condoning misconduct to meet business targets. The result is employees who can justify wrong-doing and organizations in which people do not feel comfortable reporting fraud, bribery and corruption.

The results of our 2017 survey indicate that certain unethical behaviors can be seen as acceptable in today's workforce, particularly among executives. Of our respondents in senior management roles, 44% feel offering cash payments to win or retain business could be justified, compared with 29% of all other employees. These figures are higher than those in EMEIA, where one in three board directors and senior managers say they could justify offering cash payments to win or retain business, compared with one in five of other employees.

When it comes to bringing forward sales and booking revenues early to meet short-term financial targets, 45% of senior management thought this was justified. This is substantially higher than in EMEIA, where only one in five board directors and senior managers would be willing to act in this way.

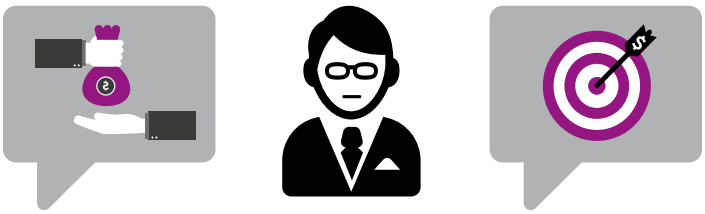
Senior managers ignoring unethical behavior

Ethical standards are not improving because employees are receiving mixed messages from management. Senior managers must consistently model, encourage and enforce compliant conduct. Yet our findings suggest this is not happening in almost half of the region's organizations. Forty-nine percent of respondents say that, even though they see senior managers saying no to bribes, those same managers would ignore the unethical behavior of employees if their actions helped to achieve corporate targets.

Our 2017 APAC survey finds that 87% of senior management could justify unethical behavior to help a business survive, compared with 77% of board directors and senior managers in the equivalent EMEIA survey. Approximately the same percentage (23%) of senior management in both geographies say they would deliberately misstate a company's financial performance.

The 2017 survey results show that, despite ABAC policies being in place, misconduct is not being reported because employees and managers still feel under pressure to stay silent. Almost a third (32%) of respondents say the atmosphere in their organization means they do not feel comfortable reporting unethical behavior – a sentiment that is felt even more keenly at the top of some companies.

Of our respondents in senior management roles



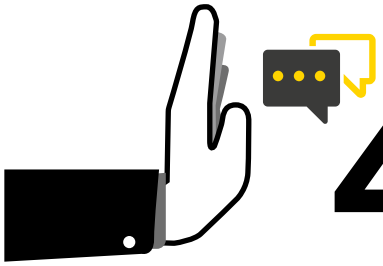
44%

feel **offering cash payments to win or retain business** could be justified

45%

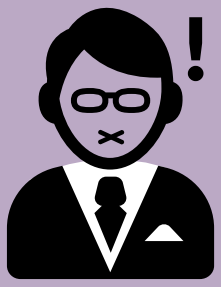
feel it is **justified to bring forward sales and book revenues early** to meet short-term financial targets

Senior management willing to ignore unethical actions of employees



49%

of respondents think that their **senior management would ignore unethical behavior to achieve corporate revenue targets**



51%

of **senior management respondents feel under pressure to withhold information** about misconduct

Two in five (41%) of respondents, and more than half (51%) of senior managers, say they have felt under pressure to withhold information about misconduct. The higher numbers of senior managers reporting this pressure may be because they are personally at risk of sanctions, or it may be that the misconduct is protecting leadership bonuses.

Tellingly, almost a quarter (24%) of respondents do not believe that management would protect people who report cases of fraud, bribery and corruption. Meanwhile, 21% believe that their organizations simply do not investigate breaches of ethical standards.

This level of mistrust is putting organizations at unnecessary risk. More than a quarter (27%) of respondents say they are aware of fraudulent activities, but don't do anything about it.

These findings help to explain why, despite investment in compliance, employees are still engaging in unethical behavior, such as paying cash to win contracts or misstating financial performance. Making ABAC policies work requires behavioral change. Unless line managers ensure people feel comfortable to report misconduct, employees remain reluctant to do so.

Lack of awareness from Gen Y

Our survey finds that younger respondents do not fully understand what constitutes unethical behavior. Even though Generation Y employees (25-34 year olds) are the group least willing to work for unethical companies, they are more likely than any other age group to be prepared to offer cash payments to win or retain business – 38% compared with 28% of all other employees. Similarly, 42% of Generation Y would extend the monthly reporting period to meet financial targets, compared with 31% of all other employees. Whereas, when provided with more clear-cut choices, such as ignoring compliance controls, Generation Y responded in line with all other age groups that, this was not justified to meeting financial targets. These findings underscore the importance of companies providing younger staff with clear guidance and ethical training. These figures are higher than those found in EMEIA, where 25% of Generation Y would offer cash payments to win or retain business and 20% would extend the monthly reporting period to meet financial targets.

Tough growth conditions used to justify unethical conduct

Just over half of our respondents (51%) believe that tough economic times are the reason for the increase in bribery and corrupt practices – and many employees are sympathetic to this view point. Asked if they personally could justify inappropriate conduct to help their business survive, more than two-thirds say they would introduce more flexible product return policies for customers. Almost a third (32%) would offer a cash payment to win or retain business. Here again, we find perceptions of leadership endorsement driving these inappropriate behaviors.

When asked whether they believed that management would justify unethical conduct to meet financial targets, 35% of our respondents say management would condone extending the monthly reporting period and 15% say management would justify deliberately misstating a company's financial performance.

We can see this phenomenon playing out in corporate reporting: 50% of all respondents believe that companies in their country often report financial performance as better than it is.

Of our Generation Y (25-34 year olds) respondents:

38%

are more likely to offer cash payments to win or retain business

42%

would extend the monthly reporting period to meet financial targets

51%

of respondents think that bribery and corrupt practices have increased because of tough economic times

Compliance weak spots emerging in sales and finance

In an uncertain, lower-growth environment, our findings reveal sales teams under pressure to manipulate sales results as well as finance teams under pressure to misstate results. Compliance teams need to act quickly to:

1. **Detect:** by using forensic data analytics to identify early warning signs, such as changes to product return policies or retrospective rebates, before events spiral out of control. What individuals may see as small, justifiable sales policy modifications, regulators could interpret as aggressive channel stuffing that fraudulently inflates revenue. This is a real danger point. If people believe the organization condones actions that improve results, they could continue to push the envelope of "justifiable" behavior toward outright fraud.

2. **Defuse:** by focusing on the positive aspects of compliance: educating employees about and incentivizing and empowering them to make the behavioral changes required. This will mean specifically linking reward and remuneration to ethical behavior. It will also involve enlisting the support of leaders, from C-suite to line managers, to communicate a "zero tolerance" attitude to compliance breaches. Business leaders will need to be open about why the organization can no longer have a sales culture that promotes "winning at all costs" and explicitly talk about what compliant growth looks like.

Unethical behaviors employees believe are justified to help a business survive.

67%

Employees believe it is justified to introduce more flexible product return policies for customers

47%

Employees believe it is justified to negotiate retrospective rebates, bonuses or discounts for suppliers

38%

Employees believe it is justified to offer entertainment to win and retain business

35%

Employees believe it is justified to offer personal gifts or services to win and retain business

32%

Employees believe it is justified to offer cash payments to win and retain business

Unethical behaviors employees believe management would justify to meet financial targets.

61%

Employees believe management would justify introducing more flexible product return policies for customers

35%

Employees believe management would justify extending the monthly reporting period

34%

Employees believe management would justify bringing forward sales and revenue

34%

Employees believe management would justify booking revenue from rebates/promotional funding deals early

31%

Employees believe management would justify changing the assumptions that determine valuations or reserves

Employees bypassing whistleblowing hotlines

Despite an increase in the uptake of and willingness to use whistleblowing hotlines around the APAC region, our 2017 survey findings indicate that many employees still don't trust that their organization will take action on whistleblowing complaints or keep them confidential.

In positive news, 10% more employees are willing to use a whistleblowing hotline than they were two years ago – 63% up from 53% in 2015. Fewer respondents are being deterred from using a hotline due to concerns about insufficient legal protection for whistleblowers (14% down from 19%) – reflecting the better protections that some governments have put in place over the last two years.

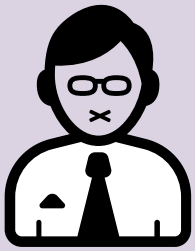
However, given the choice, only 27% of respondents would opt to report misconduct using their in-house whistleblowing hotline, with 23% preferring to go direct to senior management. In contrast, 39% would rather use an external channel, with one in five saying they would be most comfortable calling an anonymous law enforcement channel, such as the police or a government hotline.

This preference for external channels may stem from employees' lack of faith in their organization's willingness or ability to take appropriate action in relation to whistleblowing reports, or a perception that the external channel offers greater anonymity. Only 37% of respondents have confidence that a report to the company's whistleblowing hotline will always be followed up.

The fact that one in five employees would rather take a misconduct report direct to law enforcement is an alarming development. If employees don't feel comfortable using an organization's internal whistleblowing hotline, their ethical imperative to report wrong-doing is taking them direct to the authorities – with the strong potential to lead to far worse financial and reputational outcomes than internal whistleblowing.

Without an effective mechanism to support early detection, unethical behavior can take years to uncover, leading to significant corporate financial losses over time. Having strong whistleblowing programs, which are typically the first and most common line of defense, is essential if organizations want employees to report misconduct early.

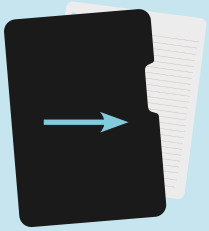
1 in 4

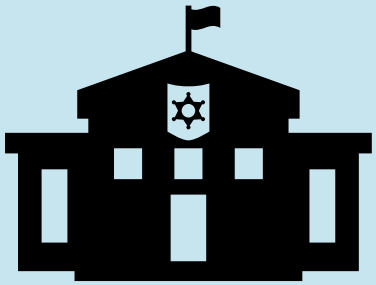


respondents say their colleagues are **aware but do not report fraudulent activities**

respondents **do not have confidence in their organization to protect them** if they report miscounduct

1 in 5





respondents would rather **take a whistleblower report direct to law enforcement**

How to improve employee trust and confidence in hotlines

▶ Make a strong commitment to confidentiality

to build trust in using hotlines. A third of respondents who wouldn't use a hotline believe their report will not be treated confidentially. Senior management must communicate regularly and with conviction that each report will be treated confidentially, without exception. Organizations should also consider outsourcing some element of the disclosure receipting process to engender greater independence and rigor.

▶ Strengthen triage and case management systems

to ensure that all complaints move through the system towards resolution and that reports are seen to be investigated. Currently, only 37% of employees believe that a report to a company's whistleblowing hotline will always be followed up. Organizations must act and be seen to be acting on every complaint. Even if, on investigation, no further action is required, this should be communicated.

▶ Introduce whistleblower champions

to raise awareness of the importance of speaking up about issues and educating employees about their options to make disclosures. An effective way to enhance awareness and encourage staff to raise concerns is by sharing success stories. For example, organizations should highlight where whistleblowing has resulted in improvements in performance, prevented health and safety breaches, or detected control gaps. The communication can be as simple as sharing key whistleblowing management information or through case studies in staff training programs.

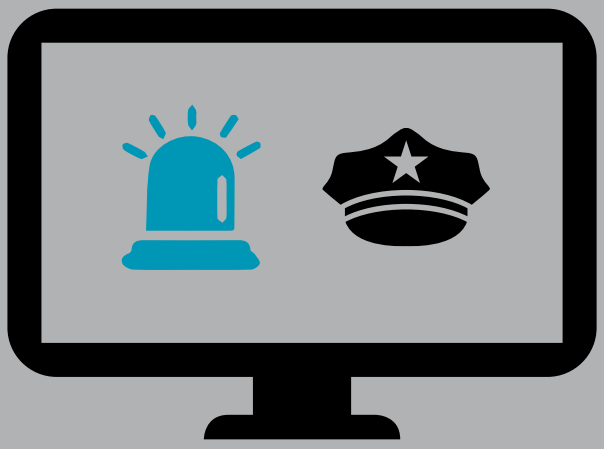
▶ Use benchmarking

to ensure best practice and effectiveness. A robust program of regular, independent benchmarking against industry peers can help organizations to assess whether a hotline is fit-for-purpose and making the best use of the latest technology, such as mobile apps. Benchmarking will examine a hotline's effectiveness considering an organization's operations, geography, industry, workplace culture, risk profile and history of known events.

Will the region's governments and regulators choose to establish financial incentives to encourage whistleblowers to come forward?

Since its establishment in the US in 2010, the SEC whistleblower program has bolstered the agency's enforcement efforts. In 2016, the agency received 4,200 tips and issued awards totaling US$57 million – higher than all the award amounts in the previous years combined.

The information and assistance provided by whistleblowers led to successful SEC enforcement actions that ordered US$584 million in financial sanctions, including more than US$346 million in disgorgement of ill-gotten gains and interest that were returned to harmed investors.



Respondents prefer to use external whistleblowing channels such as

- **Anonymous law enforcement channels**
- **Anonymous social media avenues**

"While many studies point to whistleblowing as one of the most effective means of detecting fraud, bribery and corruption, much still needs to be done to build trust in whistleblower systems. This is not simply about providing a whistleblower line; it is about building a system for whistleblowing that ensures matters are received efficiently and dealt with in a prompt, transparent, consistent and ethical manner."

Rob Locke, Oceania Leader, Forensic & Integrity Services

Compliance lacks clarity

Our 2017 survey finds that a significant number of employees misunderstand critical elements of compliance policies and processes, highlighting areas where organizations should work to clarify and raise awareness of what ethical conduct looks like. As a matter of urgency, leaders should make sure that they know the answers to the following questions.

Do employees understand your ABAC policies?

According to our 2017 survey, for the vast majority of organizations, the answer to this question is likely to be: "No."

A massive 85% of our respondents want to change their organization's ABAC policy to make it more understandable. Specifically, they think existing policies are too long and use unnecessarily complex language (including legal jargon).

Beyond simplifying and shortening ABAC policies, employees believe understanding would be greatly helped if policies are provided in the local language and explained in terms of real-world, local business examples that clearly demonstrate compliant behavior.

Almost a quarter (24%) of respondents believe their head office does not provide enough budget and decision-making authority to local business management to fight bribery and corruption in their market.

85%

of respondents want their organization's **ABAC policies to be simplified and localized** to make them more understandable

What changes would you make to your company's ABAC policy?

- **I would shorten the policy to focus on key messages**
- **I would simplify the language of the text**
- **I would localize all scenarios and language for it to make sense to our local business activities**
- **I would change all of the above**

Is your code of conduct practical?

A significant minority (39%) of respondents say their code of conduct has little impact on actual employee behavior, perhaps in part because employees either do not understand or do not see the relevance of this element of compliance. Two years ago, a majority of employees told us their code of conduct should be more flexible to accommodate local needs. Our 2017 survey finds little has changed, with 57% of respondents once again agreeing with this point. Some respondents also believe there is a disconnect between directives from head office and the realities of the local market. A worrying 14% of respondents believe that the management team at head office does not understand the local business environment.

Organizations must test their codes of conduct for local understanding and clarify as needed to fit with business practices on the ground.

39%

of respondents say that their organization's **code of conduct has little impact on how people actually behave**

57%

of respondents believe that their organization's **code of conduct should be more flexible** for local offices

Do you have a well-articulated gift giving and entertainment policy?

Our 2017 survey finds that many organizations are failing to provide adequate direction around gift giving and entertainment. More than one-third of respondents say their organization either has no gift giving policy at all, or that they have a policy but it is vague and they do not understand it. Interestingly, the majority of employees have strong opinions about what their gift giving policy should be. Almost 60% of respondents want their organization to avoid all ambiguity and provide employees with an exact monetary amount for gift giving and entertainment.

Clear policies and procedures around gift giving are essential, as temptations for bribery and corruption abound. Best practice includes:

- **Communicating a clear policy statement in the local language**
- **Setting a 'no-exceptions' monetary limit**
- **Clarifying the approval process for gifts within this limit**
- **Describing what are and what aren't suitable gifts or entertainment options**
- **Explaining in unambiguous terms the potential implications of non-compliance**

"Organizations need clear, simple policies that make it easy for front-line employees to politely decline a request for a deviation."

Emmanuel Vignal, Greater China Leader, Forensic & Integrity Services

59%

of respondents say that their organization should specify an exact monetary amount for gift giving and entertainment

33%

of respondents believe their organization's gift and entertainment policy is vague and that they don't understand it

Are you tackling the complexities of third-party risk management effectively?

Increased organizational reliance on third parties

In the two years since our 2015 survey, the ecosystem of third parties has grown more complex, as companies have changed their business models to take out costs and secure growth in new markets. With more outsourced or distributed functions, new players in their supply chains and organizational reliance on third parties has never been greater nor the risk more far reaching.

Our 2017 survey finds an increase in awareness of third-party risk – 62% up from 55% in 2015. Three in five respondents believe that third parties constitute a "significant risk" to their organization. In relation to the third parties they work with, more than 80% say it is important to understand each organization's: media coverage of fraud, bribery and corruption; past or current litigation; and its compliance culture.

Gaps in third-party risk management

Our findings suggest that, even though a majority of respondents recognize third-party risk as a concern, a significant number of organizations in APAC are still not proactive enough when it comes to on-boarding and monitoring their business relationships. Nearly a third (32%) of the respondents say their organizations do not conduct any audit reviews of their third parties or are unaware of such activities when managing existing ones. As third parties continue to be the nexus between companies and recent FCPA (Foreign Corrupt Practices Act) enforcement actions, it is critical that relationships are scrutinized with more care and consistency. Faced with limited budgets and growing number of business relationships, companies need to have a risk-based third-party management approach by categorizing each of their third parties into low, medium or high-risk entities and conduct appropriate levels of integrity due diligence to understand the compliance risks associated with new and existing business partners. Business volume, nature of the business relationship, location of operations, government interactions and history of wrongdoings are all factors that can help determine the level of risk and scrutiny required to manage third parties. If deemed high risk or if any red flags were found, a more frequent and comprehensive audit approach should be incorporated throughout the life-cycle of the business relationship. Since the level of risk may increase after on-boarding, companies need to proactively monitor their third parties by identifying changes in ownership structures or new compliance red flags. Our 2017 survey findings suggest that many organizations are neither equipped to detect changes in third-party risk conditions nor able to adapt appropriately.

As a priority, companies should harness the digitized information now available for third-party risk assessment. Organizations can use forensic data analytics to quickly transform large volumes of transactional and publicly available data into valuable actionable business intelligence. This will enable the appropriate monitoring and review of risk drivers, so that companies' compliance functions can respond accordingly.

More than a quarter (26%) of respondents do not know whether their organization is conducting compliance audits, suggesting gaps in communication around third-party risk. Assessing risk exposure requires multiple functions such as procurement, sales, marketing and legal to manage third parties in accordance with firm policy.

32%

of respondents are not aware of or do not conduct any audit reviews on their third parties

"As ethical behavior becomes a market differentiator, senior management should be more involved in conversations around third-party risk management. In today's fast-changing environment, relationships are complex and dynamic, requiring continuous third-party risk monitoring. Companies will need to leverage digital data in the most cost efficient and effective way to address key risks around third parties and their activities."

Reuben Khoo, ASEAN Leader, Forensic & Integrity Services; APAC Leader, Forensic Technology & Discovery Services

63% Vendors and Suppliers

Managing general contractor risks via compliance risk assessments

Issue	A large retailer was concerned about potential corruption risks with the general contractors building its stores.
Approach	EY reviewed procurement activities within key contracts with, project payment processes with, change orders during construction process with, bidding and selection processes with, invoice and payment processes with, and interactions with government officials relating to permits and licenses.
Findings	A number of corruption risks and control gaps were found in vendor's payments, especially around inconsistent purchase orders and questionable expenses in the contractors' payments made to local government.
Outcome	The findings were communicated via stakeholder workshops to make procurement, finance and legal teams aware of the risks. EY also developed FDA risk indicators and risk scoring frameworks for stakeholders to proactively monitor potential fraudulent vendor payments.

61% Distributors

Large distribution chains and dealer channels require a risk-based Integrity Due Diligence (IDD) approach

Issue	A medical device company planning to enter Mainland China by acquiring its largest distributor wanted to conduct IDD to understand the FCPA and reputational risks associated with this market entry strategy.
Approach	EY designed a risk-based IDD program that identified 35 out of nearly 300 sub-distributors as high risk and conducted IDDs for these organizations focused on FCPA red flags.
Findings	Many glaring red flags emerged, ranging from sub-distributors pushing sales by providing lavish gifts and vacations, to sub-distributors on government blacklists for prior corrupt conduct.
Outcome	The client terminated numerous sub-distributors and for those that remained, the client provided significant comprehensive assistance with FCPA compliance policy development and training. As a result, the client entered the market with a much larger network of distributors, confident of where the risks were and how to manage them.

High-risk third parties

63% Agents

High-risk agencies require thorough forensic third-party audits and site visits

Issue	A global pharmaceutical company operating in Mainland China wanted to assess risk around travel agencies organizing events.
Approach	Given the large number of agents involved, EY took a risk-based approach by first conducting due diligence on high-risk vendors and assessing a sample of transactions. This was followed by physical site visits and forensic reviews of selected travel agencies, interviewing senior management on compliance policies, procedures and controls, inspecting supporting documentation of the pre-selected transactions and seeking explanations of anomalies detected.
Findings	A number of questionable and sometimes non-existent events reportedly organized by the travel agencies were found.
Outcome	This exercise led to a broader and more regular review of the client's high-risk travel, marketing, public relations and government relations agencies to better identify red flags and prevent future incidents.

62% Joint venture partners

Corporate marriages mean more opportunities, responsibilities, risks and diligence

Issue	A client wanted to identify compliance red flags in relation to a planned JV with a local company (the target).
Approach	EY conducted pre-close forensic due diligence to understand the target's background and reputation, assessing its interactions with government agencies and state-owned enterprises, identifying past transactions that may have related to corrupt payments. EY also assessed the target's compliance program, tested transactions with its own third-party intermediaries and assessed its financial controls.
Findings	In addition to an effective compliance program, more significantly, we found instances of accounting fraud, evidence of potentially corrupt payments to government officials and inappropriate gift giving and entertainment.
Outcome	Now with a clear understanding of the risks, the client made the decision to walk away from this deal to find a more ethical party to work with.

Q. How significant of a risk do you think each of the following is to your business in relation to bribery and corruption?

Base: Total respondents (1,598), except India.

Spotlight on: financial services

Increasing demands of Know Your Customer (KYC) and Anti-Money Laundering (AML)

Many of the region's regulators are now requiring the boards of financial institutions to demonstrate active management of money laundering and terrorist financing risks. The result is that client due diligence now goes beyond identifying and verifying the customer. Institutions must also identify beneficial ownership and control, and conduct ongoing due diligence and scrutiny, via customer monitoring and transaction surveillance systems, throughout the course of the business relationship.

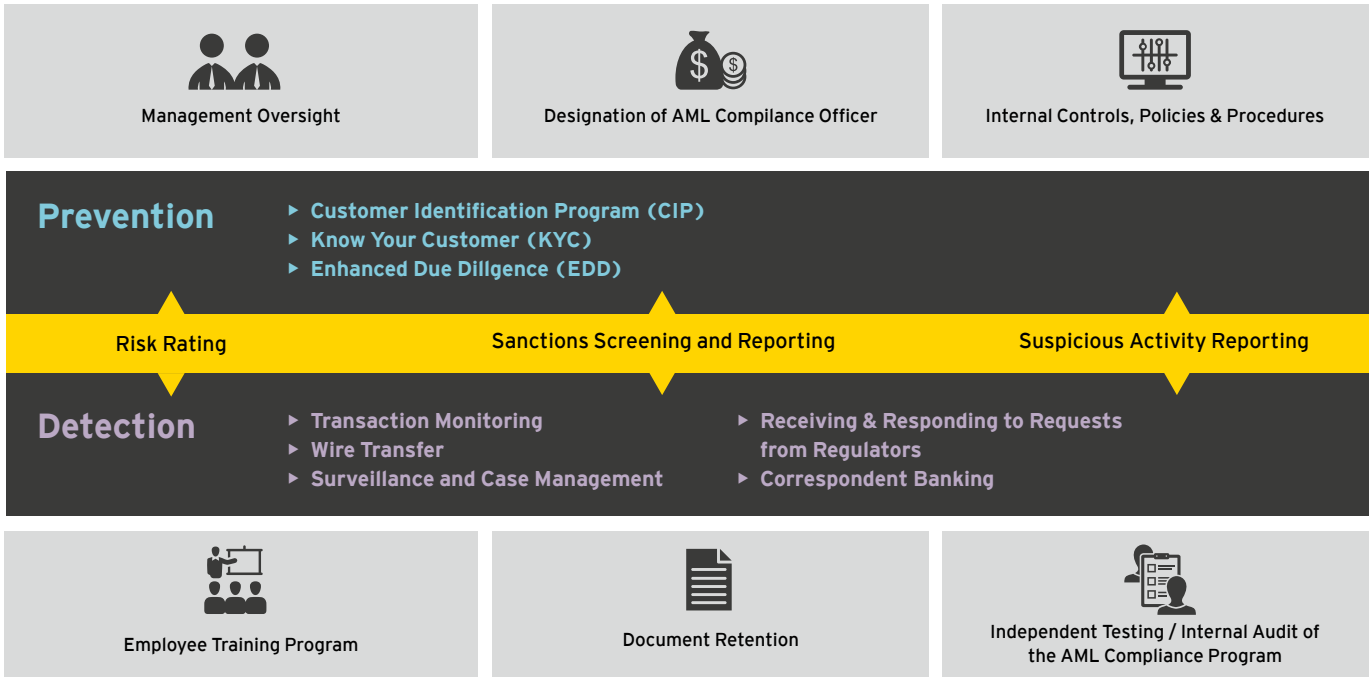
At the same time, regulators are setting higher standards of due diligence and requiring more comprehensive information on a customer's customers, including beneficial ownership information that is not currently easy to obtain in all APAC countries. Some financial institutions are struggling to fulfil these obligations, especially in terms of relying on their direct customers conducting their own due diligence around beneficial ownership.

Our survey respondents in the financial services sector report a sharp rise (46% up from 22% in 2015) in the negative impact of regulation – well above the regional average of 31%. This has required financial institutions to make significant changes to control frameworks, driving up the cost and resources required for compliance. Where increased costs have prompted institutions to outsource their onboarding or compliance processes, such arrangements must be monitored with particular care. Institutions can outsource a function, but they cannot outsource accountability.

Whether outsourcing or insourcing, financial institutions should also optimize transaction surveillance to reduce false positives. Recent regulatory actions have exposed material deficiencies in current supervision and surveillance capabilities.

Financial Institutions need to stay on top of current and emerging regulatory risks on an ongoing basis; they also need to take a holistic approach to improve their supervision and surveillance capabilities.

Essential components of an anti-money laundering program



"Regulators expect financial institutions to be responsible for maintaining a robust AML, KYC and sanctions compliance program for their entire enterprise footprint, including third-party outsourcing vendors. As such, financial institutions must ensure their outsourcing vendors can maintain the same AML compliance control standards as the financial institutions themselves."

Manhim Yu, Partner, Forensic & Integrity Services, Hong Kong

Do your employees know how to combat cyber attacks?

Growth in employee-related risk exposure

In the last two years, criminal syndicates have been increasingly targeting human rather than technological weaknesses in corporate defenses. This is why, in the 2016 EY Global Information Security Survey (GISS) of more than 1,700 chief information security officers (CISOs) and other executives, respondents rated careless or unaware employees as their primary vulnerability to cyber attack, with 55% saying this had increased their risk exposure. As a result, security awareness and training was the number one priority for increased spending on improving data security. In fact, nearly half (49%) of the 92% of surveyed CIOs and CISOs said they would spend more on training in the coming year.

Our 2017 APAC Fraud Survey findings reflect this trend, with an 8% increase in respondents who had received data security training – 63% up from 55% in 2015.

Employees underestimate cyber threats

In the wake of an explosion in cybercrime, APAC employees have a greater awareness of this issue in general than in 2015. However, they have yet to understand how great a threat cyber attacks and insider threats pose to their own organizations. Almost a quarter (24%) of employees in our 2017 survey do not know whether their organization had been a victim of cyber attacks in the last two years – only a third think they had been.

The reality is that, over the last two years, the quantum, variety and sophistication of cyber attacks have all increased exponentially. In our experience, over this time period most organizations have likely already been attacked – even though they may not know it yet. Many cyber attacks are not discovered for months and sometimes years. In one investigation of hackers who had gained access to customers' online trading accounts at a global bank, EY found user access anomalies dating back more than 12 months before the identified hacking incident.

Personal devices are an open door to cyber criminals

As a clear example of the under-estimation of cyber risk, our 2017 survey identified personal mobile devices as a specific area where APAC organizations are vulnerable to cyber breaches through their employees.

Just under half (47%) of our respondents say their organizations have no policies against using personal devices for work-related activities. Almost half of our respondents (49%) admit to conducting business using their personal mobile device, even though their organization provided them with a work mobile device – and 36% do so frequently. Worryingly, these figures are even more prevalent with senior management, 53% of whom say they frequently conduct business using their personal mobile device.

Two-thirds (66%) of respondents agree that there are risks associated with using personal devices for work-related activities, but 53% of these respondents admit they do so anyway. This highlights the issue that, even when the risks are understood, without clear and consistent policies in place, employees will often demonstrate poor judgment.

47%

of respondents say that there is **no company policy against using personal devices for work-related activities** at their organizations

> "The sheer volume and the level of sophistication of cyber attacks we see today continues to expose even the most sophisticated organizations to potential breach. It is critical that employees understand this and are educated about their role in helping to defend against the wide range of threats their company faces."
>
> **Warren Dunn, Partner, Forensic & Integrity Services, Australia**

How safe are your critical assets from insider threat?

The financial, reputational and regulatory impact of having an organization's critical assets stolen or damaged can be catastrophic. Anyone with trusted access can exploit the vulnerabilities that protect critical assets, causing millions of dollars of damage. To mitigate this risk, organizations should establish a program to protect their critical assets from insider threats.

Managing insider threat risk should be part of a comprehensive corporate security program, from both information security and physical security perspectives. However, insider threat poses unique information security challenges. For example, they:

- **Do not need to "break in" because they already have access and knowledge pertaining to the location of critical assets**
- **Are within an organization's confines, so their illicit activities are harder to detect via traditional signature-based detection than an external attacker**

Do you have a comprehensive view of risk?

Our 2017 survey finds that many organizations in APAC have a fragmented view of and approach to cyber risk. In fact, companies need to treat cyber and insider threats in the same manner – as elements of an ever-present overarching risk – requiring a comprehensive and highly disciplined risk management approach. It doesn't matter whether the threat comes from outside or inside the organization, if it is fueled by malicious intent or enabled by ignorance, the impact of an information breach can be financially and reputationally devastating.

What is insider threat?

An insider threat is when a current or former employee, contractor or business partner, who has or had authorized access to an organization's network systems, data or premises, uses that access to compromise the confidentiality, integrity or availability of the organization's network systems, data or premises, whether or not out of malicious intent. Insider threats can include fraud, theft of intellectual property or trade secrets, unauthorized trading, espionage and IT infrastructure sabotage.

66%

of respondents acknowledge that there are **risks associated with using personal mobile devices for work-related activities**

Cyber breach response program – what does "good" look like?

Given the likelihood that all businesses will eventually face a cyber breach, it is critical that APAC organizations develop a strong, centralized response framework as part of their overall enterprise risk management strategy.

Have you considered...

- **Whether your breach response plan includes all the right functions: legal, compliance and public relations?**
- **Whether your employees know whom to call when they suspect a cyber incident?**
- **How incidents are escalated within your company, who must be told and when?**
- **Whether your incident response team has segregated duties? Is the team purchasing antivirus technologies the same as the one investigating when those tools fail?**
- **Whether you have contracts in place for situations where you need outside help due to the scale of the issue or the unique skills required?**
- **Whether you have protocols for when you will notify law enforcement and regulators?**

Special feature: India

Ethical standards rising – but there is still much ground to cover

India has witnessed a transformation in its anti-corruption regime, spurred by Government initiatives, regulations and changing public sentiment. The Companies Amendment Bill 2016, which focuses on governance and ease of doing business in India, and has been an important factor in enhancing ethical standards. According to 70% of the respondents in India, such Government efforts against bribery have had a substantial impact on corporate India.

This is also reflected in respondents' views of their own organizations. India ranks the same as Mainland China with 60% of respondents stating that their company's ethical standards have improved in the last two years. However, 78% also say that fraud, bribery and corrupt practices continue to happen widely in India, followed by 48% stating that it is common to use bribery to win contracts. These findings put India above the regional averages of 63% and 35% respectively.

In line with other countries, respondents in India said they had ABAC training and policies in place. However, organizations in India still have some gaps when it comes to tone at the top and could do more to demonstrate ethical leadership.

More than half (57%) say that, even though senior management said "no" to bribes, they would choose to ignore unethical actions of employees to achieve corporate revenue targets. The sentiment was quite strong, with 23% saying "definitely yes", more than double the regional average of 11%, to senior management choosing to ignore unethical actions of employees. Almost a quarter (24%) of respondents say their organization's management would also justify ignoring compliance controls to meet revenue targets.

With 86% of respondents saying they would consider employment opportunities elsewhere if their organization was involved in a major fraud, bribery or corruption case, companies in India need to do more to strengthen their ethical leadership.

Concerns around whistleblowing mechanisms

Since the 2016 Companies Amendment Bill made setting up a whistleblowing mechanism mandatory for listed companies in India, whistleblowing hotlines have become more common. However, 47% of respondents feel under pressure to withhold information about misconduct and 44% of respondents in organizations where a hotline was in place say they would not use the system. Of these, more than half are concerned about insufficient legal protection and a third do not believe their report would be treated confidentially.

More discipline needed in third-party due diligence

More than 80% of respondents say it is important to understand a third party's ultimate owners, compliance culture and any news or litigation associating the organization with fraud, bribery or corruption. However, we still see gaps in conducting robust due diligence and monitoring.

One of the challenges is that, frequently, a public domain search in India does not reveal adequate third-party information. Organizations need to conduct field surveys and background checks to get adequate certainty around information integrity before entering into a contract, which includes audit rights to enable continuous monitoring.

Those with a complex network of third-party relationships should consider using web-based tools to standardize transparency and accountability. These tools enable life-cycle management of third parties, with automated risk-scoring engines to calculate risk according to individual organizational priorities.

> "In 2017, the battle against fraud and corruption is expected to see a tectonic shift as India strives to keep pace with global standards, drive sound governance and stimulate business growth. As enforcement actions by local authorities grow stronger and employees resist being part of unethical work environments, the future of compliance programs will become more visible, resilient and technologically-led."
>
> **Arpinder Singh, India and Bangladesh Leader, Forensic & Integrity Services**

Conclusion

Our 2017 survey finds that APAC organizations will continue to be challenged to prevent fraud, bribery and corruption in an environment of greater scrutiny. The impact of fraud is increasing on all fronts, from intensifying regulatory pressure, the increasing complexity of third-party relationships and pervasive and ever more sophisticated cyber threats. At the same time, the economic volatility that is squeezing compliance budgets is also putting management and employees under pressure, leading some to make unethical decisions in a misguided attempt to achieve better results.

Without more assertive action from boards and management to assess the risks and take robust action, we can expect more large-scale fraud, bribery, corruption and competition scandals in APAC involving major corporations.

As a priority, senior management in APAC need to undertake an urgent assessment of the spiraling threats facing their organizations and strengthen their defenses around both people and technology.

Call to action

1

Revisit ABAC policies

Existing ABAC policies should be simplified, localized and explained in terms of real-world examples. Organizations that don't have them, should introduce precise gift-giving and entertainment policies. To make policies effective, all leaders, including line managers, must proactively educate employees that compliant behavior is not a hindrance to commercial success, and incentivize and empower employees to make compliance a top priority. Managers must model appropriate behavior and give people incentive to comply with policies at all times, even if it means losing a sale. Organizations must link reward and remuneration to ethical behavior.

2

Harness forensic data analytics

Compliance teams are being asked to review an ever-increasing volume of transactions but with fewer resources and greater time constraints. FDA is key to keeping up with the mountains of data organizations must sift through to prevent and detect fraud, bribery and corruption. Compliance teams need to use FDA to monitor the full range of data points – not just looking for red flags in financial data, but for example, using sentiment analysis of emails, text and chat, where legally permissible, to detect early warning signs of misconduct.

3

Raise the bar for third parties

The region is moving at different speeds when it comes to the level of transparency and access to information about third parties. This is a challenge for businesses working in multi-jurisdictional environments and contracting across borders. As companies look to grow their businesses in the region's emerging markets, compliance programs will need to raise the bar to include multiple ABAC and anti-competition laws and regulations, especially with APAC regulators continuing to focus on the risks third parties pose to companies.

4

Benchmark whistleblowing hotlines

Benchmarking will help organizations to identify whether their whistleblowing hotline is fit for purpose, if employees are aware of, trust and use the service. This will not happen unless people feel safe reporting fraud, bribery or corruption and have confidence that action will be taken as a result. Companies must adopt and enforce policies to protect whistleblowers from retaliation. They should also implement programs to encourage employees to report unethical behavior and ensure appropriate, consistent and transparent follow-up to their disclosures.

5

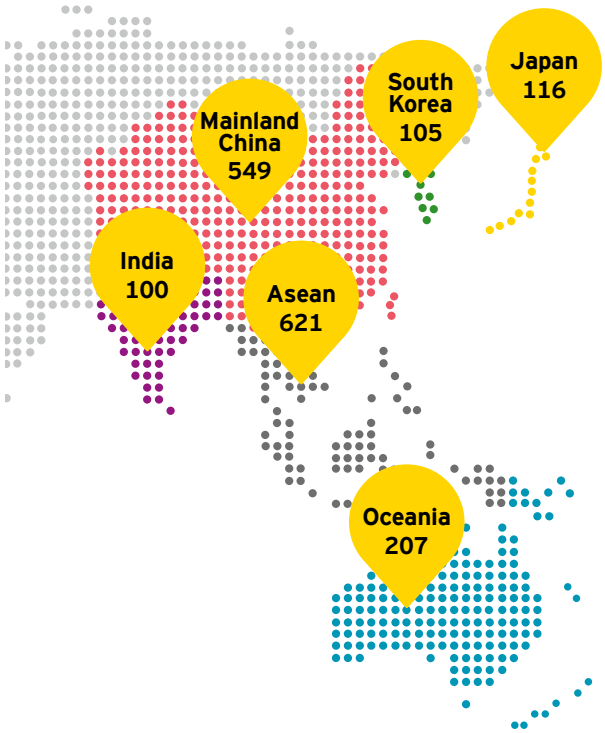
Treat data risk as one holistic program

Traditional cyber defenses are not coping with the evolving threat landscape and increased regulatory demands. Cyber criminals, hackers and malicious insiders – employees, former employees, contractors, business partners – are targeting organizations for their sensitive commercial information as well as their cash. Companies are increasingly vulnerable through careless employees and others not following technology security protocols. As a result, cyber and insider threats are part of one larger risk that will require a holistic approach for its detection, investigation and prevention.

Respondent profiles

Geographical spread

Between November 2016 and February 2017, our researchers – the global market research agency Ipsos – conducted 1,698 interviews with employees of large companies in 14 APAC territories: Australia, Mainland China, Hong Kong, India, Indonesia, Japan, South Korea, Malaysia, New Zealand, Philippines, Singapore, Taiwan, Thailand and Vietnam. The interviews were conducted online in local languages on an anonymous basis covering a mixture of company sizes, job roles and industry sectors.



Company size - number of employees globally

42% Above 5,000

22% 1,500-4,999

15% 1,000-1,499

11% 500-999

6% Less than 500

Industry sector*

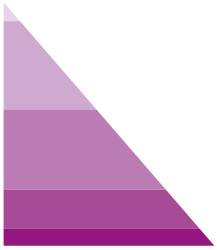
22%	Retail and manufacturing	5%	Extractive
15%	Information computing technology	4%	Transportation
11%	Financial services	3%	Hospitality and leisure
7%	Life sciences	2%	Power and utilties
6%	Professional firms and services	2%	Real estate
6%	Automotive		

*The remaining percentage of industry sector respondents not presented above relates to unspecified sectors.

Role

21%	Senior management
39%	Middle management
40%	Other employees

Age



5%	Under 25
39%	25-34
33%	35-44
16%	45-54
7%	Over 55

Contact information

The EY Forensic & Integrity Services practice has a global reach. See below for a list of our country and territory leaders.

For more information see www.ey.com/forensics.

Local contact	Name	Telephone
Global Leader	**Andrew Gordon**	**+44 20 7951 6441**
Asia-Pacific Leader	**Emmanuel Vignal**	**+86 21 2228 5938**
Americas Leader	**Tony Jordan**	**+16175851951**
EMEIA Leader	**Stefan Heissner**	**+44 20 7951 5386**
Afghanistan and Pakistan	Shariq Zaidi	+92 21 3567 4581
Argentina	Andrea Rey	+54 1145 152 668
Australia and New Zealand	Rob Locke	+61 28 295 6335
Austria	Andreas Frohner	+43 1 211 70 1500
Baltic States	Liudas Jurkonis	+370 5 274 2320
Belgium	Frederik Verhasselt	+32 27 74 91 11
Bolivia	Javier Iriarte	+591 2 2434313
Brazil	Marlon Jabbur	+55 11 2573 3554
Bulgaria	Ali Pirzada	+359 2 817 7100
Canada	Zain Raheel	+1 416 943 3115
Chile	Jorge Vio Niemeyer	+56 2 676 1722
China (mainland)	Diana Shin	+86 21 2228 2371
Czech Republic and Slovakia	Tomas Kafka	+420 225 335 111
Denmark	Torben Lange	+45 2529 3184
Ecuador	Geovanni Nacimba	+593 22 555 553
Finland	Markus Nylund	+358 405 32 20 98
France	Philippe Hontarrede	+33 1 46 93 62 10
Germany	Stefan Heissner	+49 221 2779 11397
Greece	Yannis Dracoulis	+30 210 2886 085
Hong Kong (SAR)	Chris Fordham	+852 2846 9008
Hungary and Croatia	Ferenc Biro	+36 30 567 0582
India/Bangladesh	Arpinder Singh	+91 12 4443 0330
Indonesia	Alex Sianturi	+62 21 5289 4180
Ireland	Julie Fenton	+353 1 221 2321
Israel	Ofer Erez	+972 3 6278661

Local contact	Name	Telephone
Italy	Fabrizio Santaloia	+39 02 8066 93733
Japan	Ken Arahari	+81 3 3503 1100
Kenya	Dennis Muchiri	+254 20 2886000
Luxembourg	Gérard Zolt	+352 42 124 8508
Malaysia	Joyce Lim	+60 374 958 847
Mexico/Colombia	Ignacio Cortés	+52 55 1101 7282
Middle East	Charles de Chermont	+971 4 7010428
Netherlands	Brenton Steenkamp	+31 88 40 70624
Nigeria	Linus Okeke	+234 1 271 0539
Norway	Frode Krabbesund	+47 970 83 813
Peru	Rafael Huamán	+51 1 411 4443
Philippines	Roderick Vega	+63 2 8948 1188
Poland	Mariusz Witalis	+48 225 577 950
Portugal	Pedro Subtil	+351 211 599 112
Romania	Simona Radu	+402 120 47970
Russia	Denis Korolev	+74 95 664 7888
Singapore	Reuben Khoo	+65 6309 8099
South Africa/Namibia	Sharon van Rooyen	+27 11 772 3150
South Korea	Steven Chon	+82 102 791 8854
Spain	Ricardo Noreña	+34 91 572 5097
Sri Lanka	Averil Ludowyke	+94 11 2463500
Sweden	Erik Skoglund	+46 8 52059939
Switzerland	Michael Faske	+41 58 286 3292
Taiwan	Chester Chu	+86 62 2757 2437
Thailand	Wilaiporn Ittiwiroon	+66 2264 9090
Turkey	Dilek Cilingir	+90 212 408 5172
UK	Richard Indge	+44 20 7951 5385
US	Tony Jordan	+16175851951
Venezuela	Jhon Ruiz	+58 21 2905 6691
Vietnam	Saman Wijaya Bandara	+84 90 422 6606

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services
Dealing with complex issues of fraud, regulatory compliance and business disputes can detract from efforts to succeed. Better management of fraud risk and compliance exposure is a critical business priority – no matter the size or industry sector. With approximately 4,500 forensic professionals around the world, we will assemble the right multidisciplinary and culturally aligned team to work with you and your legal advisors. We work to give you the benefit of our broad sector experience, our deep subject-matter knowledge and the latest insights from our work worldwide.

EYG no. 02079-175Gbl
ED None

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com/forensics