

Asia Pacific investigations
capability survey
Are you prepared for
the new normal?

Contents

Executive summary	03
Strategy and support	05
Structure and capability of an investigations function	06
Your investigations team	08
Whistleblowing	10
Technology and data	12
GDPR and privilege in investigations	14
The future of in-house investigations	15
Deloitte Forensic in Asia Pacific	16
Contacts	17

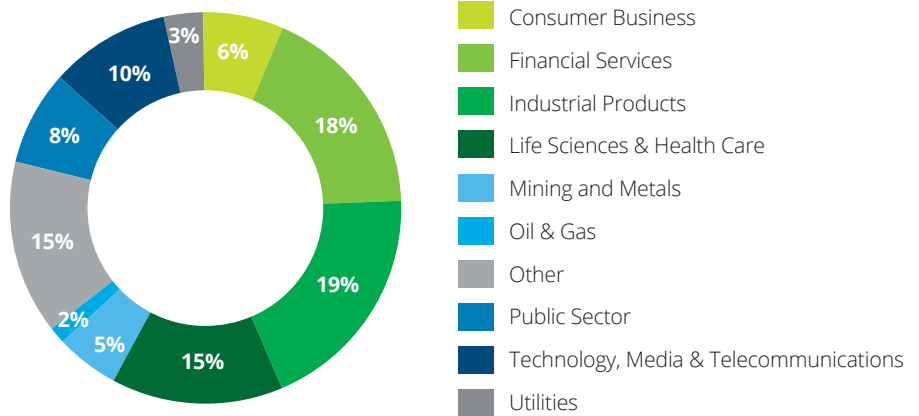
Executive summary

Culture, values and ethics are more than ever at the forefront of priorities for various stakeholders of an organisation. However, it is becoming harder for organisations to navigate this complex landscape, and the price for failing to do so is rising. With a wider group of individuals, including board members and senior management, being held accountable for corporate misconduct, organisations need to have robust processes and strong controls in place. Investigations are a key component of this, as a minimum to investigate misconduct as it comes to light, efficiently and effectively.

Previously, little work has been done to understand what the people in charge of corporate investigations themselves think about their function's role and status within the organisation. What challenges do they face, how are these challenges met, and do they feel that their role is taken seriously enough within their organisation? To discover the answer to these, we have conducted this survey in conjunction with the Association of Corporate Investigators ("ACI") across Asia Pacific with executives in this area. This report presents our findings and analysis. We suggest that it is required reading for corporate investigators and the senior executives with responsibility for them. This will help them understand the common weaknesses, and best practice, of this vitally important function.

Our survey was conducted in the last quarter of 2020 with 62 executives across the Asia Pacific region. The respondents were from a range of industries comprising of senior employees from Compliance, Investigations, Legal, Risk and Internal Audit functions.

Respondents by industry



Key insights:

Nearly two-thirds of respondents are not confident or neutral that their investigation capabilities adequately cater to the risks their organisation faces.

An investigations function needs to be dynamic by having an overall purpose and strategy to ensure effectiveness in understanding, evaluating and responding to risks faced by the organisation.

26% of respondents think that the current structure of their investigations function is not effective in conducting investigations, while 27% are neutral.

Factors that contribute to an investigations function being ineffective include lack of influence and resource and cost limitations.

Only 19% of organisations are confident that their current training programme meets the needs of their investigators. Reasons include the content not being detailed or lacking industry specific content. Organisations may want to consider other supplementary avenues for training to address this, including an accredited corporate investigator training programme. The ACI is currently developing foundation qualifications for the corporate investigator.

Only 23% of respondents said that people within their organisation feel comfortable in 'speaking up' in respect to the actions of peers or superiors and only 42% feel comfortable when it concerns employees in junior roles. This may indicate a lack of confidence by employees in their organisation's whistleblowing process due to either inaction from management or fear of retaliation. An independent and objective investigations function can play an important role in promoting a culture of speaking up by demonstrating timely and objective follow-up of complaints and helping to ensure appropriate safeguards are in place to protect the identity of the whistleblower.

Whilst most organisations surveyed are either already using or are considering using data analytics as part of their investigative work, **only 19% said that their data analytics capability was mature.** In order to generate the required insights from an investigation and with increasing volumes of data, investigations functions should look to expand their data analytics capabilities, including scalability of current systems to handle big data.

Strategy and support

Strategy of an investigations function

Only 36% of respondents are confident that their current investigation capabilities will adequately cater to the risks faced by their organisation, 32% are not confident and the rest are neutral. This is particularly concerning. If an investigations function is not dynamic, the ability to understand and evaluate risks faced by the organisations may be impaired, together with the capability to carry out an appropriate and timely response.

Whilst thorough planning is clearly essential for an investigation, having an overall purpose and strategy are essential for an effective investigations function. Without this, the day-to-day operation of the investigations capability and making effective decisions is harder to manage, let alone planning and making decisions on investment. A clear strategy and purpose will also keep talented people motivated, and more willing to stay with the organisation.

Strategy can be significantly impacted by areas such as regulatory changes and external threats (e.g. cyber-crime) and becomes even more relevant in today's volatile economic climate arising from the COVID-19 pandemic. It is critical for organisations to assess if new and evolving risk areas have been mitigated.

Senior management support

Overall, 68% of respondents think that their investigation mandate is supported by senior management. Of the 21% who feel unsupported by senior management, we found that they also do not think the strategy and direction of their investigation function will address the needs of the organisation in the future.

We observed a correlation with senior management support and whether the organisation measures the success of its investigations. All respondents who felt unsupported by their senior management also did not think that their respective organisations measured the success of their investigations.

Demonstrating the value of an investigation function to senior management and stakeholders is often challenging. It is not uncommon to see investigation support being called upon at the "11th hour", when there are expectations from regulators, or after a

"An investigations policy that clearly defines what the investigative process is, how the process will be conducted and what it means for those involved will only be successful if it has the full support of an organisation's senior management group. Without this, the integrity of an investigative process is susceptible to criticism."

Corporate Investigations Lead, Global Mining Company, Australia

significant amount of senior management time has already been diverted into managing the aftermath of an incident. Often investment in investigation capabilities is triggered by crisis, rather than occurring routinely.

In our experience, demonstration of value to senior management and business stakeholders is something investigations functions have struggled with. As we discuss below, we believe a gradual move by investigations functions to a more proactive approach to the identification of misconduct will offer additional opportunity to evidence value alongside other indicators such as highlighting risk and control recommendations and enhancements, successful case completions and where relevant, asset recoveries.

Proactive monitoring

18% of respondents say they do not consider preventative or proactive measures at all as part of their investigation function's monitoring activities, while 53% spent less than 25% of their time on such activities. This is despite the obvious benefit of identifying misconduct at an early stage before it causes significant financial or reputational damage.

Proactive monitoring, combining human expertise and data analytics to identify and investigate issues as they arise has the ability to empower investigators and help the investigations function demonstrate the value that they add to the business. Moving towards proactive monitoring will also enable investigations functions to be more insight led as well as adding an element of deterrence.

Structure and capability of an investigations function

65% of respondents have a dedicated investigations function. This number is not a surprise as large organisations would be generally expected to. However, 52% of respondents from organisations with fewer than 5,000 employees do not have a dedicated investigations function. We expect this to change as stakeholders (regulators, shareholders, employees and society at large) have increasing expectations on how organisations govern their business and respond to misconduct.

Interestingly, 26% of respondents do not feel their current structure is effective in conducting investigations, 47% think it is effective and 27% are neutral. It is unclear why over a quarter of respondents feel they are ineffective. These responses may reflect a number of factors such as historic organisational structures, stakeholder expectations and influence or resource and cost limitations.

Centralised versus decentralised investigations teams

63% of respondents stated that their investigation capability was centralised in one function, 22% said it was decentralised with the remaining 15% having a mix of both. Those respondents with a centralised structure also leveraged other functions to conduct investigations on their behalf.

In the case of a decentralised investigation capability, resources were situated across functions such as Internal Audit, Legal and Compliance. In some circumstances, specialised resources were used to meet a specific requirement(s) of an investigation. For example, a cyber-security expert may be required to handle system-related breaches.

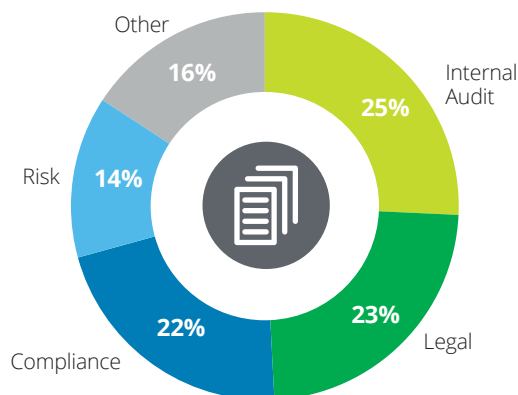
This diversity of structures is not a cause for concern – in our experience, different structures can work as long as the critical success factors are in place across the investigative governance and lifecycle from triage and accountability through investigative approach to resolution, close down and consequence management.

A case management tool (“CMT”) can act as a facilitator in addressing these factors. However, our survey noted that 66% of respondents do not have a dedicated CMT. A robust CMT enables an investigations function to identify and prioritise crucial cases, assign clear responsibility to a case investigator and store all the evidence related to the investigation in one central place. This data repository can be used as an audit trail and provide preventive insight by recognising patterns and connections and make it easier to extract statistics on investigation portfolio status to show to senior management. An integrated CMT can also guide the investigator through the investigation methodology and process for each investigation undertaken.

To whom does an investigations function report?

The survey indicated that for an investigation capability that was centralised, the function reported to either Internal Audit, Compliance, Legal or Risk. In the case of a decentralised capability, more than half of respondents noted that each function which investigates holds its own separate investigation mandate. The variety is consistent with the lines of defence.

Functions to whom centralised investigation function reports



What are the three lines of defence?

The three lines of defence is a widely acknowledged and used governance framework to manage organisational risks. The framework suggests distributing responsibility between different functions of the business to effectively manage risks.

Line	Function
1st	The function that owns and manages risks (i.e. the process owners). It is their primary responsibility to identify risks related to day-to-day operations and implement corrective controls.
2nd	The function that provides oversight over risks through developing and implementing compliance frameworks, policies and procedures. An example is the compliance department.
3rd	The function that provides objective and independent assurance that the first and second line of defence are operating efficiently. This function generally reports to the governing body (e.g. the board or the audit committee). An example is the internal audit department.

Where should an investigations capability sit?

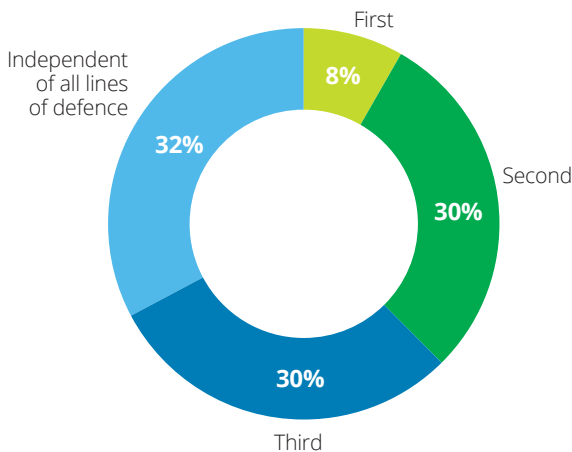
92% of respondents, most of which have an investigation function that is centralised, stated that their investigation capability sits either in the second, third or independent of all line of defences, and the remaining 8% said it sits in the first line of defence.

The first line of defence is considered inadequate as there is a lack of operational independence both actual and perceived. Typically in large organisations, the investigation capability sits within second or third line of defence. Being in the second or third line of defence allows operational independence and removes biases. Investigations can be conducted objectively and it also allows for appropriately challenging other parts of the business.

A key factor for the success of an investigations function is the ability to work independently and objectively. One way to achieve this could be for it to sit in the second line of defence with a 'dotted' reporting line to the chair of the Audit Committee, independent of both the business and the third line assurance function. Having defined areas of responsibility and an escalation mechanism within the lines of defence allows an organisation to be transparent and prevent incidents from being overlooked.

The decision not to investigate may have serious consequences in the light of subsequent events and must be appropriately documented. Given the importance of allocating investigation matters to the right team within an organisation, we typically observe specific nominated stakeholders working together and being responsible for triage and the investigations function should play a leading role in this governance process.

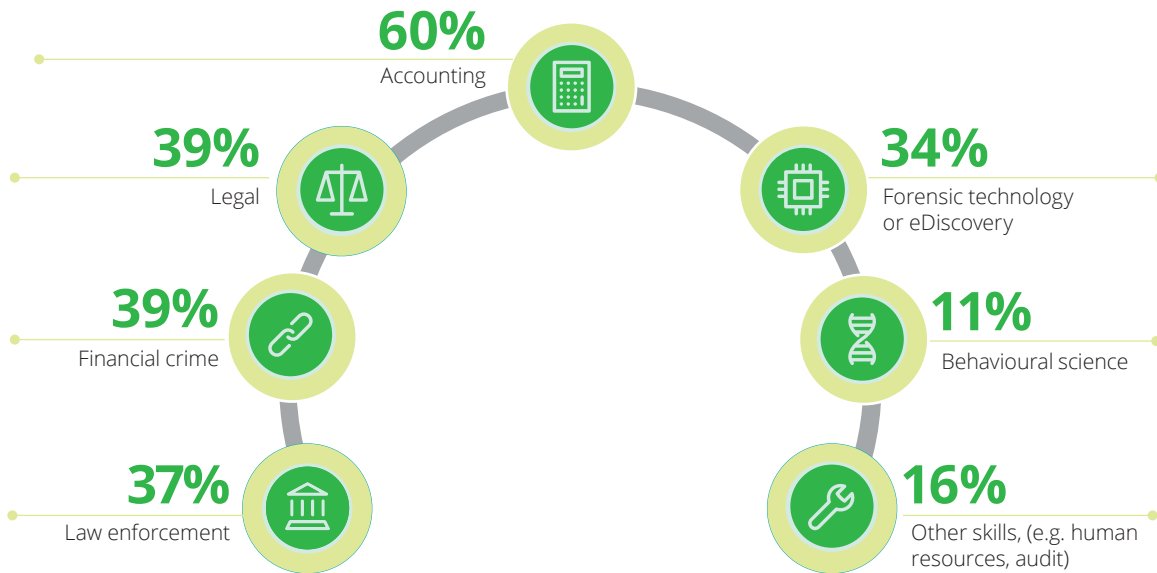
Line of defence the investigation capability is situated



Your investigations team



The vast majority of respondents have a mix of skills within their investigations functions. The most common skills for investigations functions are:

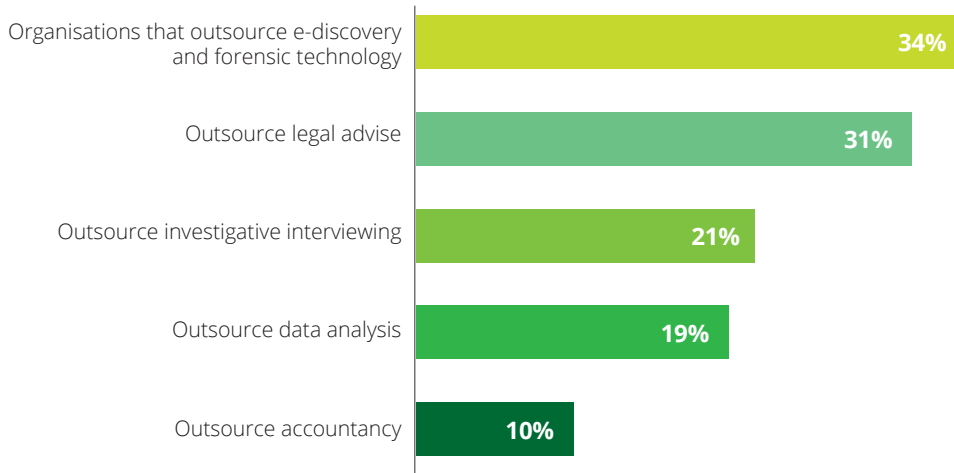


The mix of skillsets likely reflect the nature of the investigations being undertaken by different investigations functions, be that more behaviour/code of conduct focused or more focussed on money laundering or financial matters.

Across many investigations functions, we note that skills are moving beyond only having professionals with accounting, legal or law enforcement backgrounds. Investigators now have the opportunity to use more technology in their investigative activities, be that analysis of unstructured or structured data. The diverse range of skillsets is necessary in order to provide assurance to stakeholders that high quality and consistent investigations are undertaken, particularly when an organisation has a global or regional footprint. The investigator of the future will be one who can combine investigation expertise and technology analytics skills.

Outsourcing

Whilst many choose to have a range of specialists in-house there are also a number of organisations that regularly outsource elements, or all, of the investigation process to third parties. 65% of the respondents said they outsource some or all elements of the investigation.



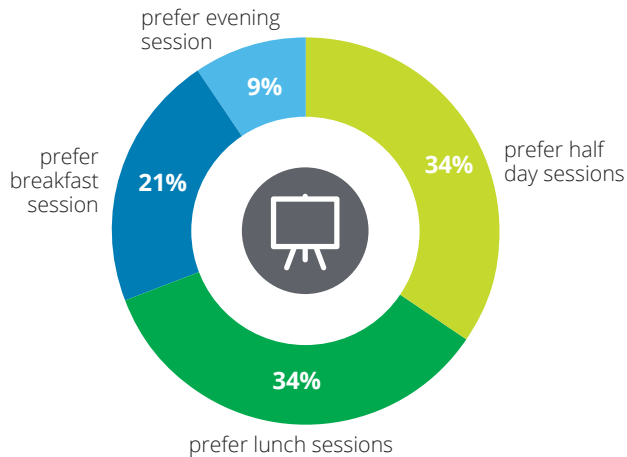
In our experience, organisations typically outsource for reasons including a large-scale investigation, need for an independent investigation, where they lack resources or need specific expertise not available in-house.

If co-sourcing is done well, the organisation has access to specialist resources which can provide scalability to the investigations function as and when required. Using a mix of internal and external specialists can reduce fixed costs, whilst ensuring that the organisation has the right skills and capacity to investigate issues as they arise.

Training

60% of respondents have a training programme for their investigations team, however, only 19% are confident that the current programme meets the required training needs.

39% stated that “industry specific content” would help, while 34% stated that their training programme needs to be more detailed. Types of training requested includes interviewing, procurement investigations, regional investigation/case trends, privilege issues applicable to Asia Pacific and compliance program grading and assessment.



Whistleblowing

Whistleblowing

92% of respondents said that their organisation has a defined whistleblowing policy. However, 15% of respondents were unsure if their organisation has an internal mandatory reporting requirement for allegations/incidents for potential misconduct and 5% said they do not have such a requirement.

Whilst whistleblowers are typically employees of the organisation, in some cases they can also be customers, suppliers or third party vendors dealing directly with employees. Whistleblowers are important given they may be closer to operational activities and therefore likely to be the first to observe any misconduct. In some cases, they are also the victims of the misconduct. Whistleblowers enable an organisation to detect incidents at an early stage and safeguard itself from losses arising out of such incidents.

89% of respondents have a whistleblowing platform, of which 44% say that the platform is managed by a third party. Of those who had a platform, we found, on average that 31% of their investigation cases originated from the whistleblowing hotline and that the top origin of investigations (40%) was noted to be internal sources.

It is generally accepted that organisations with a whistleblowing platform detect fraud quicker than those without one. Organisations should maintain multiple reporting channels such as a telephone line, web-based electronic forms and applications, emails and mailed letters to remove any barriers or impediments for potential whistleblowers to raise a concern.



Whistleblowers are important in enabling an organisation to detect incidents at an early stage and safeguard itself from mounting losses arising out of such incidents.

Whistleblowing and cultural nuances in Asia

Of concern, only 23% of respondents said that they are confident when it comes to reporting actions of peers or superiors whilst only 42% felt confident of reporting matters related to employees in junior roles. 48% of respondents said that they are confident that people within their organisation feel comfortable in 'speaking up' in respect to the actions of an external third party that may impact the organisation.

Cultural nuances in Asia may make employees shy away from reporting misconduct when it relates to their superiors or peers. There are tendencies towards group loyalty and avoiding conflicts. For example, in family-owned business and hierarchy driven structures, employees often do not challenge their peers or superiors even when they witness actions that are ethically wrong. This is due to fear of retaliation or isolation within the organisation.

The same is relevant for multi-nationals operating in Asia as local employees may feel unprotected from retaliation and isolation from headquarters. These culture nuances may create a gap in expectations from headquarters, where management depend on employees to raise concerns so that the company can take appropriate action.

“I have found that the most important drivers behind whether staff tend to speak up or not relate to the corporate culture of the organisation itself (e.g. regular, open, positive support from management) and whether the whistleblower truly believes that their identity will be protected.”

Executive Director - Investigations, Global Financial Services Company, Singapore

To overcome this challenge, management support in creating awareness and a culture of integrity plays an important role. In creating a culture of integrity, organisations need to invest in reinforcing topics such as business integrity, managing conflicts of interest and recognising and reporting behaviours that are not deemed acceptable. There are several ways management can build employee confidence to use their whistleblowing hotline to report misconduct in good faith. On top of having an anonymous reporting channel, some of the additional features that can help are:

- Taking timely action to conduct an independent and objective investigation;
- Updating the whistleblower on progress and outcome of the investigation;
- Supporting the whistleblower by positively acknowledging their complaint; and
- Positively reinforcing such actions in the organisation's public forums.

Crucial to these objectives is promoting an atmosphere where employees feel safe to engage in honest communication by raising concerns without fear of retaliation.

To enable a culture of “speaking up”, management need to look beyond simply having a whistleblowing platform as a tick in the box. Understanding the workings and effectiveness of the hotline are critical. The investigation or compliance functions can generate and analyse monthly activity reports such as number of complaints received, number of cases assigned, timeline and outcome of the investigations. The lack of hotline activity may not always be a sign that everything is intact in the organisation and is potentially indicative that employees are either not aware or confident of using the whistleblowing hotline. Other criteria to look at is the time taken to initiate and conclude an investigation after the complaint is received. Often, inaction from management reduces the confidence of employees in lodging a complaint.

Technology and data



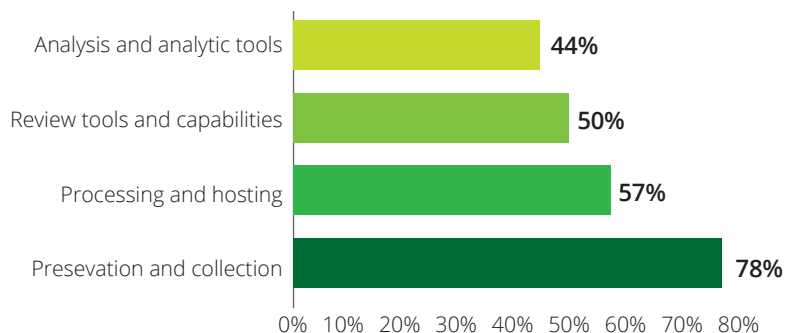
Global data volumes in business continue to grow exponentially and so investigations are increasingly becoming driven by technology and data. Data sources are critical (e.g. emails, mobile chats, video surveillance) and thus preservation of evidence is a fundamental step for any successful investigation. To prevent evidence from being destroyed, overwritten or tampered with, having a robust data preservation policy is a necessity. It simply cannot be an afterthought but the survey noted that 11% of respondents do not have a data preservation policy and 13% are unsure if one exists in their organisation.

Forensic technology

In the survey, we noted that many organisations still use traditional ways such as manual review of hard copy files (print-outs and native file/email only review) to conduct review of electronic documents during an investigation. As the volume of data grows, the traditional ways become challenging due to the structure of data, diverse sources and maintaining audit trails. Building in-house capabilities can prove to be expensive due to the high cost of technology and training required.

Whilst 89% of organisations reported that they have in-house technology capabilities ranging from preservation and collection to review and analyse, only, 33% have in-house technology support for end-to-end review. Often, organisations rely on external service providers with the required expertise to handle investigations involving large volumes of data as they are more cost-effective and able to deploy experienced resources using the latest technology.

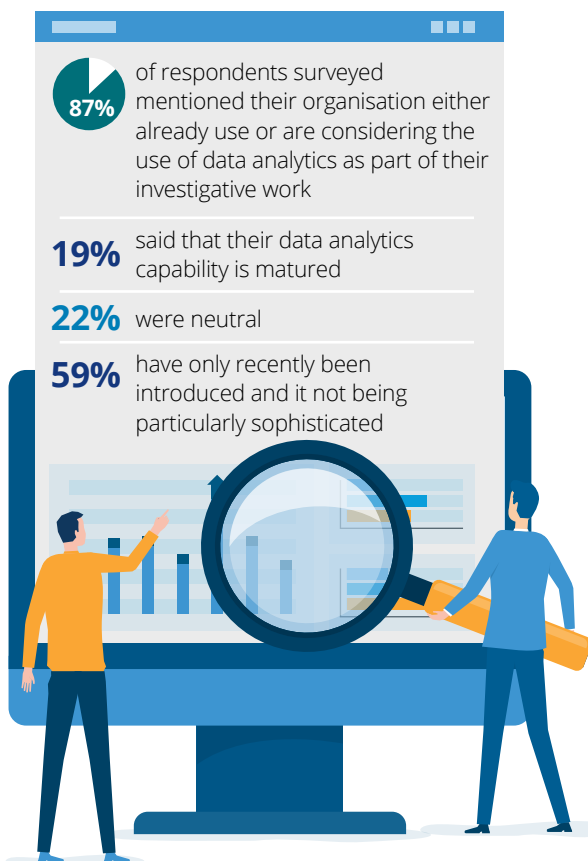
Inhouse forensic technology capabilities



“With more types of data being collected across various enterprise platforms, it is important to rely on data analytics to help holistically assess risk and investigate effectively. This is also an expectation from enforcement agencies.”

Compliance Counsel, Global Life Sciences & Healthcare Company, China

Data Analytics



52% of respondents stated that the key benefits of using a data analytics programme are early detection of fraud and detection of new fraud schemes. In this regard, we note different risks may require different analytical approaches. For example, clustering and anomaly detection use statistical profiles to identify normal activity and then differentiate outliers from these profiles. Supervised modelling in contrast uses prior economic crime, waste, abuse, and misconduct to enable the computer to “learn” the characteristics of these events, to provide early warning signs, and to identify other instances of similar behaviour.

As complexity associated with big data grows and at the risk of overwhelming the investigator, investigations functions need to consider the scalability of their data analytics capability. More powerful tools and/or artificial intelligence (“AI”) capabilities will be required. At present, 70% of respondents said that they still use spreadsheets to conduct data analytics; with only 22% using cloud or big data; 19% using machine learning/AI and 30% using a proprietary analysis platform.

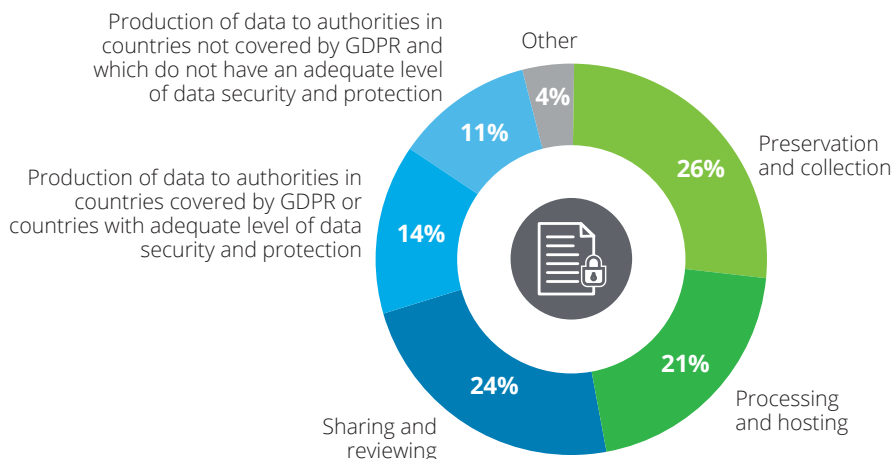
A digital and data driven operating model is a desirable state for organisations and this needs to flow through to the investigations function. Organisations need to tap the full potential of their data to gain insights from their investigations and mitigate the risks which may trigger the misconduct.

Understanding the full data landscape

Understanding the data landscape of an organisation can be a significant challenge for the investigations function. Often the information is stored in different systems which may not be inter-connected at an organisation level, particularly for multi-nationals. This could be due to different size of businesses, past mergers and acquisitions, or local regulations. This disconnect could affect the consistency and efficiency of investigations. Therefore, it is important for an investigations function to keep up-to-date with the data landscape of its organisation to ensure that relevant data sources are identified and accessed timely and the investigation plan is developed to address data sharing, transfer and review limitations caused by any relevant data privacy requirements.

GDPR and privilege in investigations

Data privacy



The General Data Protection Regulation (“GDPR”) in the European Union (“EU”) came into effect on 25 May 2018 and transformed the way we collect, use, store and dispose personal data. The requirement of GDPR not only looks at breaches but also at the overall strategy and governance of an organisation towards handling personal data. Non-compliance to GDPR will expose an organisation to financial, operational and reputational risk. While GDPR is an EU legislation, it will apply to all global businesses which manage or handle an EU citizen’s data.

Only 37% of respondents feel fully confident in determining how to deal with GDPR considerations as part of an investigation, with 48% partially confident and 15% not at all confident.

Together with GDPR, organisations in Asia Pacific have to consider data privacy regulations across the region when conducting investigations. For example, China is to enact a new data security law that may require organisations to relook how they handle and share data relating to national security, confidential business and personal information. Similarly, Vietnam is also developing a data protection decree as sub-legislation to their Cybersecurity Law for the protection of personal data.

The challenge faced by organisations is keeping abreast of new regulations as they arise across Asia Pacific and understanding how they will affect their investigation data protocols and sharing of data across different jurisdictions.

To overcome this challenge, organisations can prepare themselves by creating a roadmap to transition from their current operational and technological capabilities to new infrastructure that incorporates any required data protective measures. The three key steps in this process would be to:



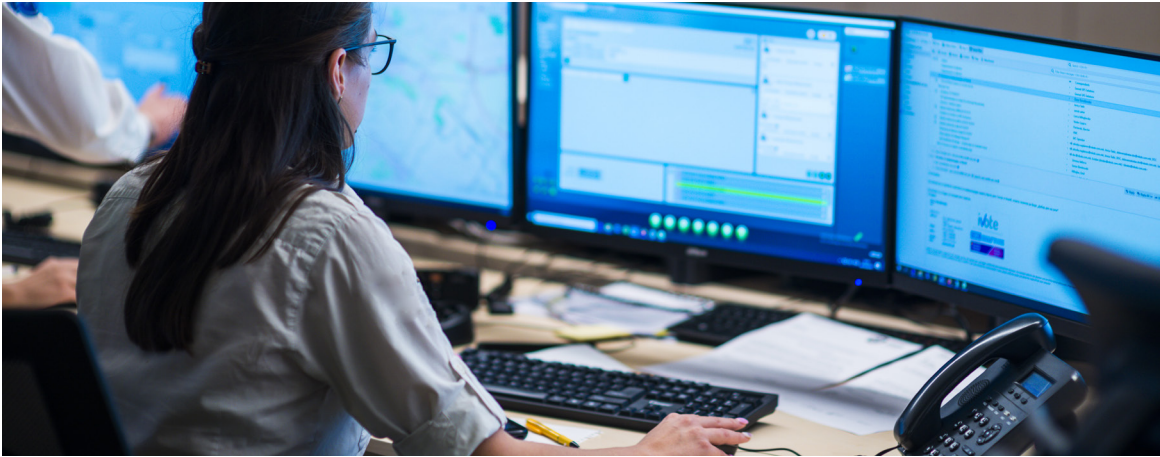
Seek professional advice at an early stage on applicable data regulations and how to tackle differences between local regulations;



Perform a current-state assessment to identify potential gaps and non-compliance with existing regulations; and



Design and implement measures to prevent non-compliance using risk-based approach.



Privilege in investigations

For investigations that could have a regulatory or external legal impact, the preservation of legal privilege will need to be considered. In some circumstances, where an investigation is being undertaken in the contemplation of litigation, litigation privilege may apply. Legal privilege may also be required for investigations across multiple jurisdictions.

In our survey, only 6% of respondents conduct their investigations entirely under privilege, whilst 21% said that none of their investigations are conducted under privilege. These responses may be reflective of the diverse legal systems in Asia Pacific where certain countries do not recognise the concept of privilege.



Whilst 44% of the respondents surveyed operate in a regulated sector, many of these organisations are conducting the majority of their investigations without legal privilege. Not using privilege may expose an organisation to the risk of disclosing information and documents that may result in greater liability; whereas overuse of privilege may attract scrutiny from regulators due to an organisation potentially being perceived as non-cooperative. Clearly, a balance needs to be struck as both the extremes can be detrimental to an organisation.

The future of in-house investigations



Just over a third of respondents are confident that the strategy and direction of their investigation capability will cater to the risks faced by the organisation. This is a worrying statistic. It suggests that investigative capabilities will need to evolve to ensure that organisations can respond to issues as they arise. It will be an even harder challenge to get to the point where they can add value to the organisation by being proactive.

In our experience many investigations functions have often grown organically over time in response to business needs, rather than in a planned way. As a result, in many cases investigations functions have never truly assessed the efficiency and efficacy of their operating models, or really considered defining and communicating their purpose, strategy and scope. They need to do this, to maximise their value to the organisation.

The changing nature of the environment within which organisations operate in Asia Pacific and heightened public scrutiny mean that having investigative capabilities within an organisation is now part of 'business as usual'. This provides a perfect opportunity for investigations functions to transform themselves into critical cogs in their organisation's prevention and monitoring strategy, to ensure the organisation can live up to its values and uphold the right culture.



Association of Corporate Investigators

"The ACI's vision is that corporate investigations is universally recognised as an accredited profession and that the ACI is a key enabler for continued personal development and operational investigative excellence"

The Mission of the ACI is to:

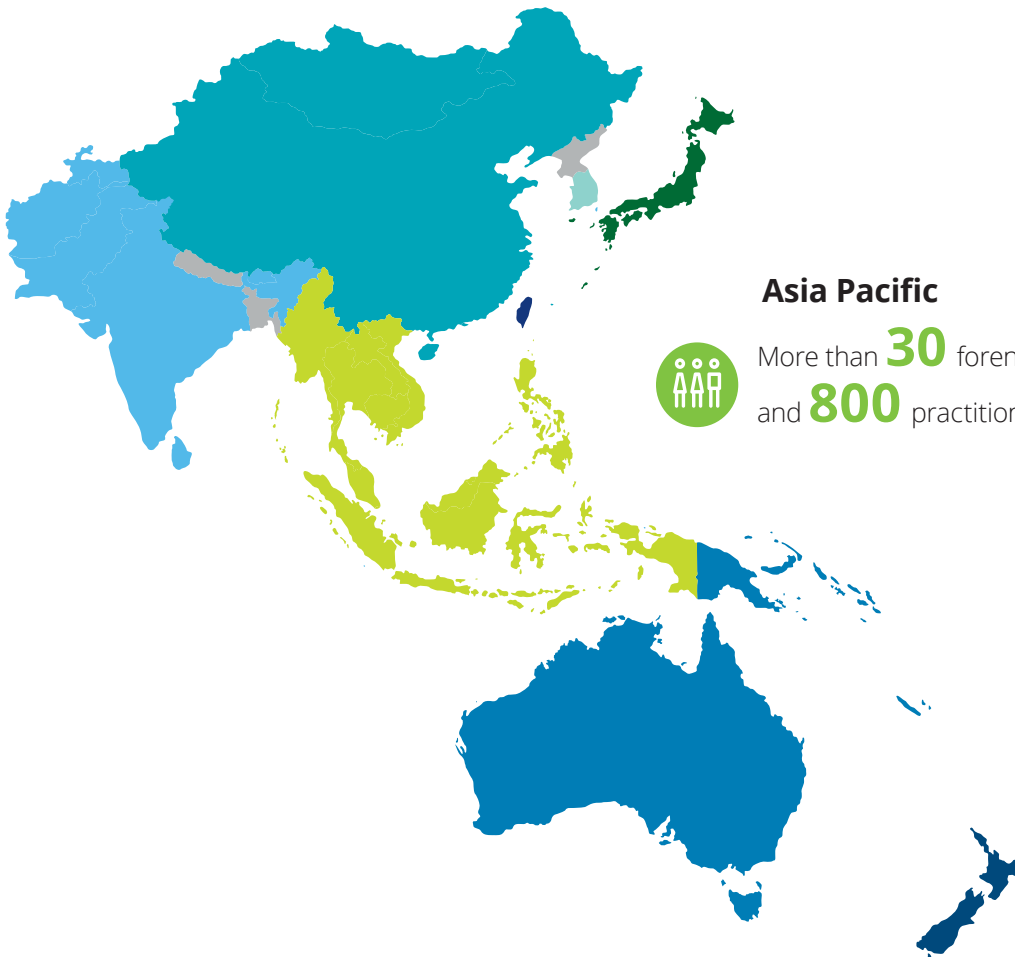
- Support professional development of members, including accredited qualifications, training, cross-industry insights on corporate investigations programmes and access to a knowledge resource centre
- Promote the highest ethical standards, including an ACI members' code of conduct
- Bring together the corporate investigations community to share best practice
- Develop a detailed accreditation program that will enable ACI members to certify with a professional investigation standard.

Deloitte Forensic in Asia Pacific

Deloitte Forensic helps clients react quickly and confidently in a crisis, investigation or dispute. We use our global network, deep industry experience and advanced analytical technology to understand and resolve issues. And we deliver the proactive advice clients need to reduce the risk of future problems.

Our services include:

- **Financial crime advisory**, assisting our clients to proactively manage risks such as bribery, corruption and other financial crime.
- **Forensic digital**, using our global digital transformation platform and networked ecosystem to deploy our current leading edge solutions and create new ones for clients.
- **Discovery**, leveraging our global industry and technical experience to create a more intelligent approach to discovery. In turn, this allows us to help address matters in a more cost-effective and robust way.
- **Disputes and litigations**, working with organisations and their lawyers in complex judicial and alternative dispute resolution matters. Our work includes deep expert witness, financial analysis, damage quantification and discovery capabilities.
- **Investigations and remediations**, in which our global network allows us to combine an understanding of local business cultures and regulatory issues to find a path to a successful resolution, and leave the client better prepared to protect their assets and reputation.



Key contacts

Deloitte Forensic Asia Pacific

Singapore

Jarrold Baker (Author)
Partner
jarbaker@deloitte.com
+65 6800 3858

Australia

Chris Noble
Partner
cnoble@deloitte.com.au
+61 7 3308 7065

India

Nikhil Bedi
Partner
nikhilbedi@deloitte.com
+91 22 6185 5130

Malaysia

Sasikala Kandiah
Director
skandiah@deloitte.com
+60 3 7610 8435

Taiwan

Kay I. Yang
Senior Manager
kaiyang@deloitte.com.tw
+886 227259988

China

Chen Zhou
Partner
zhouchen@deloitte.com.cn
+86 21 61411358

Indonesia

Winawati Widiana
Partner
wwidiana@deloitte.com
+62 21 5081 9205

New Zealand

Lorinda Kelly
Partner
lorkelly@deloitte.co.nz
+64 44703749

Thailand

Surasak Suthamcharu
Partner
ssuthamcharu@deloitte.com
+66 20340137

Hong Kong

Guy Norman
Partner
guynorman@deloitte.com.hk
+852 28521055

Japan

Yusuke Nakashima
Partner
yusuke.nakashima@tohatsu.co.jp
+81 8044351535

South Korea

Baek Chul Ho
Partner
cbaek@deloitte.com
+82 2 6676 2250

Vietnam

Santosh Balan
Director
sbalan@deloitte.com
+84 28 710 14548

Association of Corporate Investigators

Mark Gough

ASPAC Regional Head
Association of Corporate Investigators
mark.gough@my-aci.com
+61 459 340 634
www.my-aci.com

Bruce Forbes

ACI Representative Hong Kong
bruce.forbes@prudentialplc.com

Jason Landers

ACI Representative Australia
jason.landiers@riotinto.com

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms, and their related entities (collectively, the “Deloitte organization”). DTTL (also referred to as “Deloitte Global”) and each of its member firms and related entities are legally separate and independent entities, which cannot obligate or bind each other in respect of third parties. DTTL and each DTTL member firm and related entity is liable only for its own acts and omissions, and not those of each other. DTTL does not provide services to clients. Please see www.deloitte.com/about to learn more.

Deloitte Asia Pacific Limited is a company limited by guarantee and a member firm of DTTL. Members of Deloitte Asia Pacific Limited and their related entities, each of which are separate and independent legal entities, provide services from more than 100 cities across the region, including Auckland, Bangkok, Beijing, Hanoi, Hong Kong, Jakarta, Kuala Lumpur, Manila, Melbourne, Osaka, Seoul, Shanghai, Singapore, Sydney, Taipei and Tokyo.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited (“DTTL”), its global network of member firms or their related entities (collectively, the “Deloitte organization”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser.

No representations, warranties or undertakings (express or implied) are given as to the accuracy or completeness of the information in this communication, and none of DTTL, its member firms, related entities, employees or agents shall be liable or responsible for any loss or damage whatsoever arising directly or indirectly in connection with any person relying on this communication. DTTL and each of its member firms, and their related entities, are legally separate and independent entities.