



Swiss Investigations Capability Survey – Assessing maturity levels

July 2021

Content

Introduction and Context	03
Executive Summary	04
What is the purpose of investigation?	05
Strategy and Governance	06
Investigations Team	07
Privilege and GDPR considerations in investigations	09
Speak Up Lines	11
Technology and Data	13
Training and Development	15
Deloitte Forensic in Switzerland	16
Contacts	17

Introduction and Context

In mid-2020, Deloitte Forensic Switzerland, in conjunction with the Association of Corporate Investigators (ACI), undertook a survey of corporate investigators across the breadth of Swiss industry and commerce.

Our aim was to better understand the level of maturity amongst Swiss investigation functions, considering their nature and make up, how they are organised, their reporting lines, their capabilities and how those working in investigations believe their work impacts the rest of the organisation.

Our intention with this survey was to focus on those investigators based in and working in Switzerland, and to understand whether the local legal and regulatory environment affects how investigations are conducted.

We focussed our questions on several key aspects of investigations functions, namely:

- The functions strategy, purpose and risk;
- The size, capability and set up of the investigations function;
- Policies and processes including the use of Speak Up lines and GDPR considerations;
- The use of data and technology in investigations; and
- Whether required training and development needs are met.

The range of matters which an in-house investigation function may be called upon to investigate continues to be ever expanding, ranging from cyber incidents to data leakages to “me too”/discrimination issues to issues throughout a business’ supply chain. In order to continue to keep pace with an expanding investigations remit, investigation functions need to constantly develop and have an eye to the appropriate skills and experience mix required to address such a diverse range of topics.

The broadening of issues for which an investigation function may be called upon to handle is, in part, driven by the wider corporate social responsibility agenda which has become increasingly important in recent years. There is definitely an increased focus, and public scrutiny of companies, judging them not just on their financial results but also on how they interact with their customers and suppliers, what their environmental impact is and their stance in respect of human rights issues, amongst other concerns.

In Switzerland specifically, we saw the human rights topic right at the top of the political agenda in late November 2020, with a vote on the Swiss Responsible Business Initiative. The initiative sought to improve human rights and environmental protections under Swiss law and would have meant that Swiss based companies were liable for any damage caused by any companies they have control over unless they could prove they had performed sufficient due diligence procedures.

Whilst this initiative was not successful in obtaining a majority vote, there is now an alternative proposal which seeks to ultimately reform the Swiss code of obligations and criminal code by introducing duties of transparency for non-financial matters and due diligence and transparency duties with respect to minerals and metals from conflict zones and child labour. Whilst not immediately directly affecting investigation functions, there is nevertheless a clear indication that the public increasingly holds corporates responsible for their wider actions. Such increased scrutiny in those areas will undoubtedly lead to more time needing to be dedicated to these topics by investigation functions in the future.

The impact of Covid-19 on investigation functions

It is difficult to reflect on findings from a survey conducted during 2020 without considering the impact of Covid-19 on investigation functions. Unquestionably, investigation functions have had to adapt

in the short term, pivoting themselves to conduct investigations remotely, including performing interviews online rather than in person, leveraging data and technology in different ways or making use of personnel from other departments due to their geographical proximity to the issues being investigated. Equally any investigation function that relies heavily on Speak Up lines as sources of information may have found the number of issues reported has declined given people are working remotely and have less opportunity to overhear or observe wrongdoing or misconduct.

What is yet to be seen is the longer-term impact of Covid-19 on the way in which investigation functions will need and choose to operate. Will there be a return to the old status quo with investigations teams reverting to interviewing in person, flying in to locations around the globe when an issue arises? Perhaps more likely is a blended approach which will see investigation functions continuing to utilise some of the Covid-19 enforced practices as part of their wider and continuing suite of investigative tools. That said, for many companies who have witnessed the cost savings that are possible using technology based enablers in their investigative work, there may be an accelerated investment in technology assets, as they seek to further capitalise on the added benefits that can be drawn from the use of data analytics to inform and direct investigative priorities.

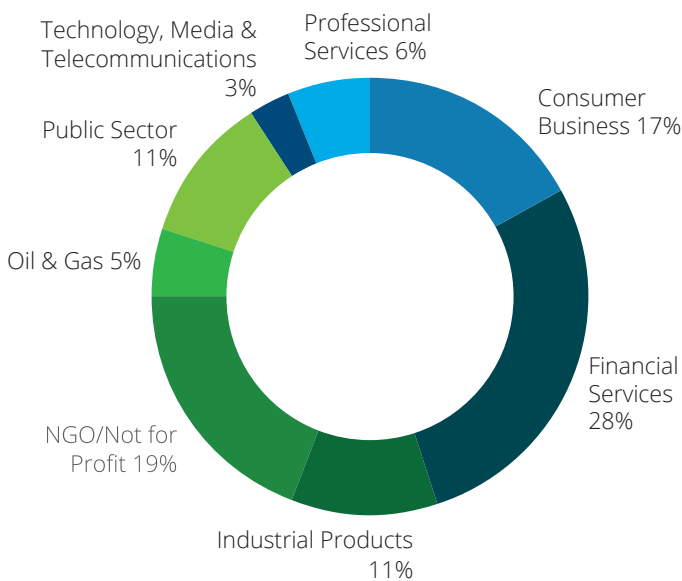
"I am delighted Deloitte have partnered with the ACI. The results provide much needed insight into corporate investigations capabilities in Switzerland. The Swiss corporate investigations community will find the results interesting as they identify areas for improvement and focus. The ACI will be taking the findings to deliver training and resources to further build on promoting best practice and investigative excellence."

Steve Young

Chief Executive Officer
Association of Corporate Investigators

Executive Summary

We surveyed 45 key executives holding positions ranging from Head of Investigations, Head of Compliance, to Head of Legal, from Swiss based companies in the second and third quarters of 2020. The majority of the respondents came from the financial services, “not for profit” and consumer businesses sectors, followed by industrial products and the public sector.



Whilst the investigation functions surveyed are based in Switzerland, many are part of large global organisations and hence the operations of the investigations function are necessarily influenced by global trends and regulations and not just by Swiss ones.

Our survey clearly shows that, as expected, there are varying levels of maturity amongst in house investigation teams. Many investigation teams now possess the capabilities to cover many aspects of an investigation, for example including the technological /data management elements. Some more developed functions have evolved from being solely a reactive force put into action in crisis, typically viewed as a cost for the business, to being able to demonstrate their value by providing lessons learned, feedback loops to the business and to compliance departments in order to prevent future incidents.

We note that our data did not demonstrate that any one industry had investigations capabilities which were consistently more mature than others. Rather there are variations in the level of maturity across companies with some appearing more advanced in one area compared to their peers but nevertheless with areas where they could develop.

There are still areas where investigation functions can increase their capabilities, be that in the skills/experience mix within the team (specifically in the areas of data analytics, technology more

widely and financial crime), providing feedback on investigative outcomes on a regular basis, and helping to reinforce a strong ethics and compliance culture.

We also noted that the remit of investigation functions is an ever widening one, and with that investigation teams will need to keep pace, upskilling their employees and leveraging technology enablers to facilitate focussed, cost effective and efficient investigative processes.

Key insights include

Strategy, Governance and Purpose

- 73% of respondents think their investigations capability has a clear strategic purpose that is linked to their code of conduct and values.
- 27% of respondents say their investigations capability has no articulated strategy.

Investigation teams

- Two thirds of internal investigation teams are centralised.
- Respondents reported 50% or more of their teams were women.

Privilege & GDPR considerations in investigations

- 4% of all respondents perform their investigations entirely under legal privilege.
- 20% say that none of their investigations are performed under legal privilege.
- 40% of all respondents feel fully confident in determining how to deal with GDPR in investigations.
- 28% of respondents noted that they consult with internal and external counsel and the respective data protection officer with respect to GDPR concerns.

Speak Up

- 84% of respondents had a Speak Up (or Whistleblowing) Policy.
- 72% of respondents have a Speak Up line in their company and of these, half are managed internally.

Technology and Data

- 84% of respondents have in house tech capabilities to support investigations.
- 52% outsource their forensic technology or e-discovery needs.

Training and Development

- 40% of all respondents have a formal training programme for their investigators.
- 48% are unsure if the requisite training needs are being met.

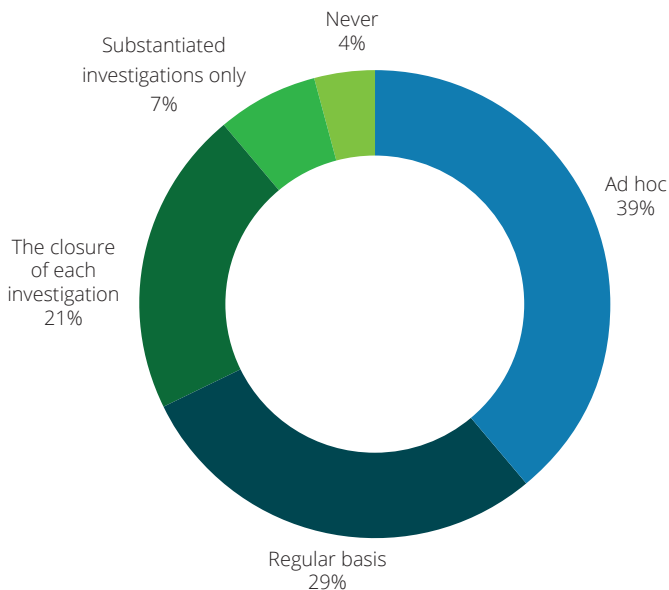
What is the purpose of an investigation?

Unsurprisingly, the majority of our respondents identified that the main purpose for an investigation was to investigate the facts and circumstances.

In Switzerland, many of the main industries are heavily regulated, notably financial services and life sciences; therefore, perhaps it is not surprising that almost half our respondents indicated that complying with regulatory/legal requirements drives the need for investigations. Likewise, many Swiss businesses have a global presence and are therefore exposed to the risk of regulatory oversight and intervention from other jurisdictions. We saw this during the last years, most obviously in financial services with the U.S. Cross Border Tax investigations, which affected many institutions in Switzerland and kept investigation functions busy for months, if not years.

With other more recent corruption scandals touching Switzerland such as 1MDB, Petrobras and Odebrecht, we note that regulatory requirements continue to be a key driver for investigations across various industry segments.

Perhaps as a consequence, not least due to the regulatory pressure to demonstrate improvements in internal controls, some 40 percent of our respondents also noted that providing a preventative and corrective capability was a key driver for their work.

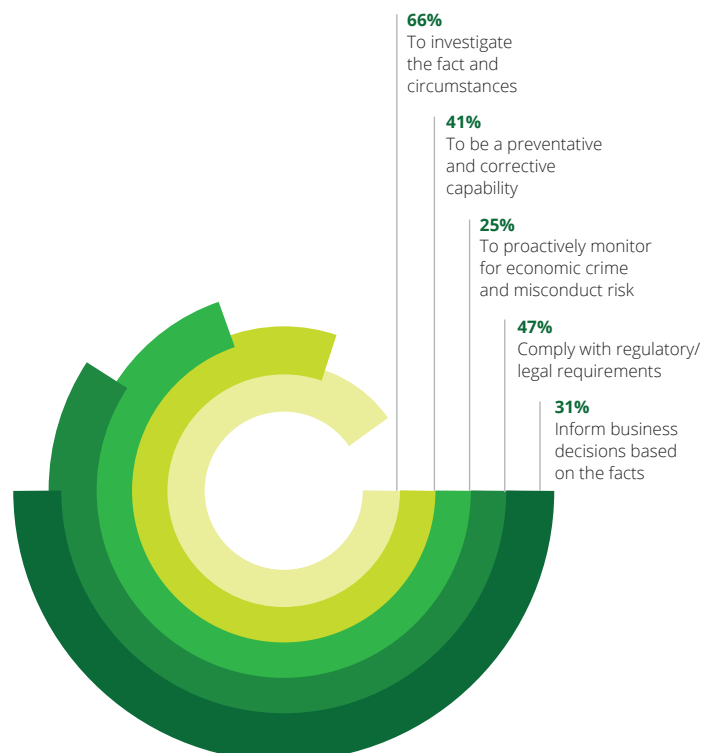


Equally half our respondents stated that they report lessons learned as the result of an investigation on a regular basis or at closure of each investigation. However, it is surprising that nearly 40% of respondents share lessons learned on an ad hoc basis only. There is a clear opportunity here for internal investigations teams to communicate lessons learned on a more timely basis in

order to drive improvements in the wider control environment. For example by closing gaps in processes which have been identified during the investigation. Sharing this information on a regular basis can help to avoid the business suffering from multiple instances of the same fraud. Regular communication of investigative findings and lessons learned may also bring wider benefits, including for example increasing confidence in Speak Up lines and making improvements in corporate culture if employees are aware there are consequences for misconduct.

We note though that only a quarter of our respondents indicated that their purpose is to proactively monitor for economic crime and misconduct risk. Whilst proactive monitoring may traditionally be seen as the responsibility of compliance functions, there is an increasing expectation that there is a collaboration between those investigating issues and those who seek to prevent them. Lessons learned from investigations, understanding loopholes which have been taken advantage of, sharing details of which data sources aided the investigation can assist the compliance function in improving monitoring. With ever increasing amounts of data available and investigation teams investing in in-house capabilities to manage and analyse this data, we expect to see more data led proactive monitoring for economic crime and misconduct.

A third of our respondents stated that they use their investigation results to inform business decisions. We expect this number will rise in the future with the increasing analysis of data that will be undertaken proactively by investigation functions.

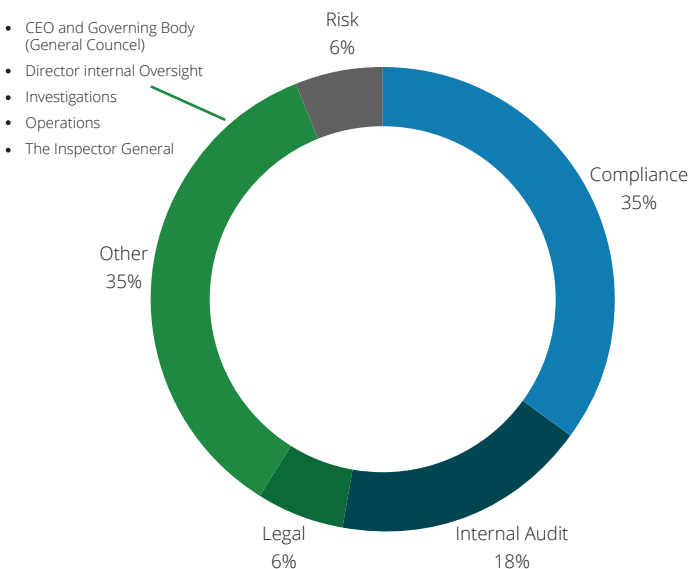


Strategy and Governance

As discussed above, most investigation functions were primarily focussed on investigating facts and circumstances. We found that 73% believed that their investigations capability has a clear strategic purpose linked to their organisation's code of conduct / values. Conversely some 15% felt that their investigation function had a clear strategic purpose, but that it was not directly linked to their organisation's code of conduct and 12% reported that their investigation function did not have a clearly articulated strategy. Having a clearly defined and articulated strategy linked to the organisations wider code of conduct can clearly benefit investigations functions in ensuring that they are focussed on investigating key risks and areas of concern for the business. Not only are they focussed on the key areas but the function is better positioned to demonstrate their value to the business if their goals are aligned with the wider business culture and ethics.

To whom does an investigations function report?

Encouragingly the overwhelming majority (85%) of our respondents felt that their investigation functions' mandate was supported by senior management. Having the support of senior management and a clearly articulated strategy can help to enforce the importance of the investigations function within the organisation.



For those with a centralised operating model most reported into compliance, followed by internal audit, risk or legal. Our respondents reported that they had direct reporting lines to various bodies, predominantly the board of directors, the audit committee, the Head of Internal Audit, the Head of Ethics / Compliance and the Head of Legal. Half our respondents reported to just one of these bodies, whilst the remainder had reporting lines into a combination of these function heads.

Three lines of defences

The 'three lines of defence' model is widely used in organisations to manage risk effectively by distributing responsibility between functions of the business.

Regardless of whether the investigation function was centralised or decentralised, most operated within the second line of defence (whose responsibility it is to set policies and frameworks and monitor compliance with them), with around twenty percent being in the third line of defence (typically Internal Audit where risk based approaches to risk management are applied), closely followed by those who reported to be operating independently of all lines of defence. Notably 15% reported that their investigation function sat in the first line of defence (i.e. the operational part of the business). This is certainly not typical and we believe may inhibit the function's ability to maintain independence in completion of its remit.

How do investigation functions demonstrate value to the business?

When it comes to demonstrating the value of the investigation function to the wider business there was no clear definitive method adopted. Most respondents appear to use a combination of methods, including providing lessons learned to internal audit and compliance, contributing to preventative methods, provision of management information, provision of training on fraud risks and recovering funds.

We noted that only 27% of respondents reported that they measure the success of investigations and each measured in slightly different ways, some considering speed at which investigation was closed, some looking at recoveries made. This is perhaps not all that surprising since it is hard to quantify what a successful outcome is for an investigation. One way in which investigation functions can seek to close this gap is to provide a feedback loop to the business in terms of lessons learned or to measure whether there is a reduction in the recurrence of similar issues over time.

"Today's state-of-the-art corporate investigation function is not just an efficient fact-finding body; it is closely connected with internal audit, risk and compliance and leveraging technology and data to inform business decisions and prevent misconduct risk. While sharing relevant observations and lessons learned are important, corporate investigation functions can add even more value when they are not working in a silo and understand their company's organization and business."

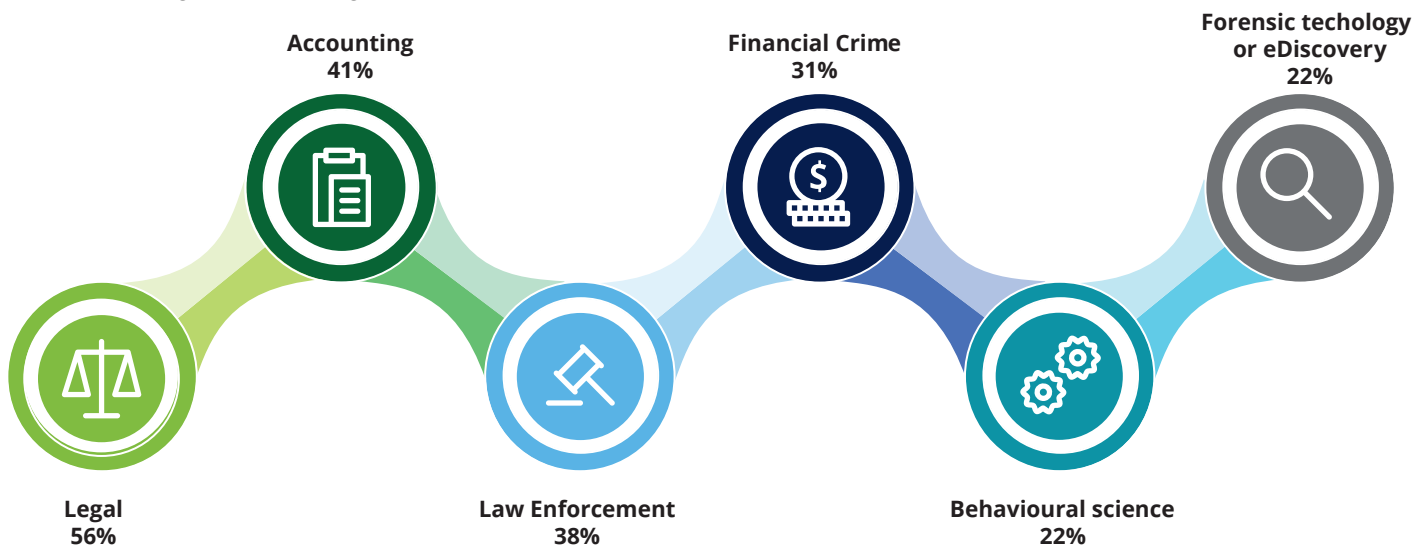
Robert Braun

Head Litigation
Novartis International AG

Investigations Team

What appears common amongst the investigation functions surveyed is the breadth of skills and experience within the respective teams: a clear majority of teams were noted to include colleagues with legal backgrounds, accounting skills and law enforcement experience. Surprisingly forensic technology or eDiscovery skills are least frequent with only 20% of investigation functions having this capability. This is especially surprising given the increasing reliance on the use of data within investigations and the fact we noted that many investigation functions reported that they could cover many aspects of the data journey in-house. We suggest, perhaps that these technology practitioners may sit within other parts of the organisation and their skills are drawn upon by the investigation function when needed.

We also note that financial crime skills and experience was only considered present within the investigation function in a third of cases. This may be a reflection of the fact that anti money laundering activities are still typically considered to be the responsibility of compliance rather than sitting with the investigation function.



Centralised or Decentralised

Approximately two thirds of respondents reported that their investigations function is centralised.

For those operating under a decentralised operating model, the investigations function tended to draw from resources across internal audit, legal, risk with some teams also utilising resources from security and HR.

Centralised teams predominantly consisted of fewer than five people, with 29% having teams of between 5 and 20 persons. Whereas for decentralised investigation functions, team sizes tended to be larger, with only 30% having fewer than five people and 60% having teams of between 5 and 20 people, with the remaining 10% having more than 30 people in their team. This may indicate that those with decentralised functions draw on resources utilising skills as needed and where perhaps those people contributing to investigations also spend their time on other work, i.e. they are not wholly dedicated investigators.

Half our respondents reported that 50% or more of their investigation team were women, with 35% of investigation functions having 50% or more of their women taking up senior leadership positions within their team.

Outsourcing

The majority of respondents outsource at least some elements of investigative, technical capabilities or legal expertise, which illustrates that many organisations may still lack the technical knowledge and legal expertise needed for a thorough investigation. Investigation functions tend to use external providers for legal advice and for eDiscovery or other forensic technological support. This is perhaps to be expected given that legal privilege may well be required for certain types of investigations, especially in the case of involvement of regulators. Furthermore, as noted in our commentary on technology, the ever-evolving data and technological landscape means it is a challenge for investigation functions to keep pace and may therefore choose to rely on external support.



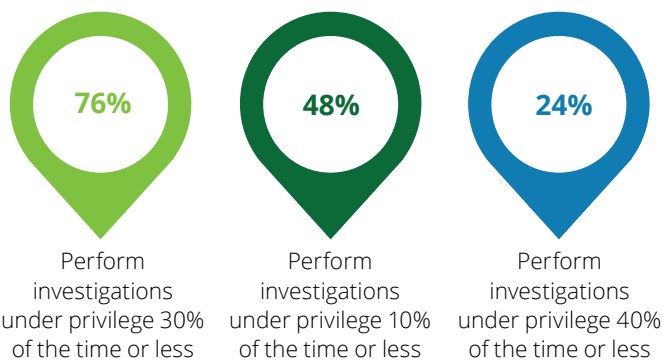
There appears to be a balanced approach adopted, having a core set of skills internally, and sourcing external support as and when needed, allowing the organisation to manage its fixed costs.

In some instances, the choice to outsource investigations is driven by geographical presence, where for example the organisation itself does not have investigations experts in certain jurisdictions. This may have become a more important driver for outsourcing during Covid-19 when investigation teams could not travel as freely as they had done previously.

Privilege and GDPR considerations in investigations

Legal Privilege

For investigations that could have a regulatory or external legal impact, the preservation of legal privilege always needs to be considered. This is where the client has a right to have their communications with their legal counsel kept confidential. In Switzerland, legal privilege does not apply for in-house legal counsel and in those investigations where it is deemed necessary or advantageous to have legal privilege, outside counsel support is required. Legal privilege may also be required for investigations across multiple jurisdictions, in which case US privilege is one of the key aspects to be considered.



In our survey, only 4% of respondents conduct their investigations entirely under privilege, whilst 20% said that none of their investigations are conducted under privilege. Respondents who answered that most of their investigations are conducted under legal privilege also tended to have investigations with high regulatory or external legal impact.

Interestingly only 16% of respondents reported that the sole reason they would appoint external counsel was to secure legal privilege. That said, 56% of our respondents noted that at least half of the time obtaining legal privilege was their reason to get support from external legal counsel. While we can say legal privilege remains a topic we can also say that it is not the main driver to engage external counsel.

GDPR

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 GDPR requirements not only look at data breaches but also at the overall strategy and governance of an organisation towards handling personal data. Non-compliance with GDPR can expose an organisation to financial, operational, reputational risk and can even trigger investigations itself. While GDPR is EU legislation, it will apply to all businesses internationally that manage or handle an EU citizen’s data and is therefore also applicable for many Swiss companies.

In addition, at the end of September 2020, both chambers of the Swiss Parliament approved the revised Federal Act on Data Protection (“FADP”), which brings the Swiss law closer to GDPR. At this point in time it is still to be determined when the new FADP will come into effect, most likely in 2022. Therefore we believe there will only be an increase in the relevance of GDPR and FADP for Swiss companies in general and in particular as a consideration for investigations functions especially when responding to multi-jurisdictional issues.

We are encouraged that 48% of the respondents feel comfortable to deal with GDPR considerations as part of an investigation and only 12% not at all.

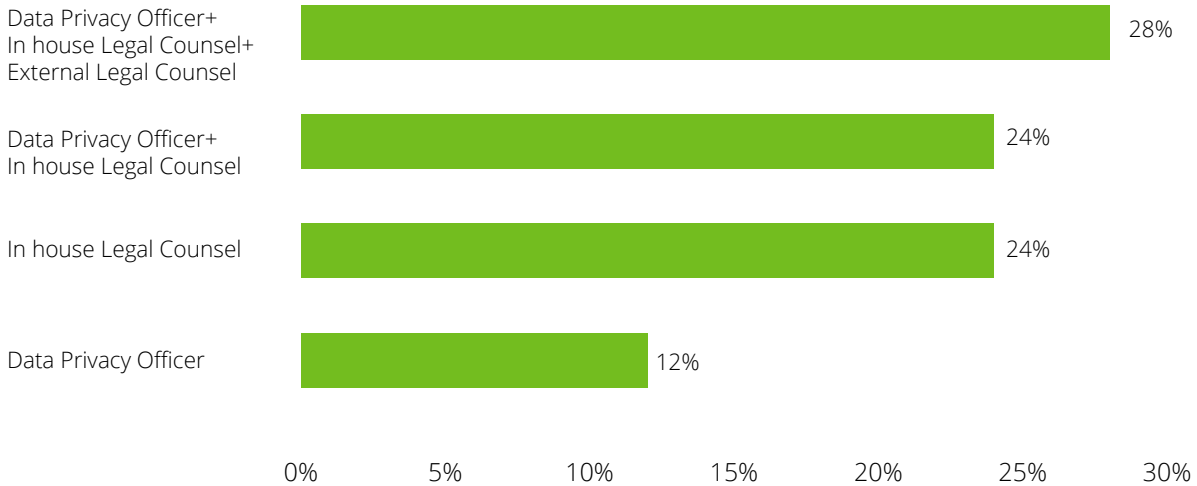
Those investigators working in the Consumer Business and Financial Services industries tended to be most comfortable with GDPR considerations. From our experience, these industries tend to be quite developed as they often operate on a global scale and are highly regulated.

We also noted a correlation between those investigation functions who conduct multi-jurisdictional investigations and the level of confidence to deal with GDPR aspects of the investigation. For those respondents who said 50% or more of their investigations are multi-jurisdictional, 100% felt partially or fully confident in dealing with GDPR.

57% of the respondents who answered that their investigations are not multi-jurisdictional at all, also feel confident regarding GDPR aspects. Whereas those with between 10% - 30% of their investigations being multi-jurisdictional seem to be less confident. It appears that those who have not yet had to deal with GDPR aspects as part of multi-jurisdictional investigations may feel confident because they have had limited exposure to the complexities of sharing data cross border. Whilst those who have had some experience are conversely less confident because they are aware of the potential challenges but have not gained sufficient experience to feel that they are fully equipped to manage GDPR in investigations.

Respondents with a Legal (38%) and professionals with a Law enforcement experience (42%) within their investigation function tend to have fewer problems dealing with data privacy considerations as part of investigations. This is further reinforced when we consider whom investigation functions consult on data privacy and GDPR considerations.

With whom do you consult on data privacy/DGPR considerations?



In house legal counsel seems to be the first go-to person for data privacy questions. However, we also see that given the complexity of the topic, 28% of respondents noted that they usually align the needs of the investigation and data privacy matters with internal and external counsel and the respective data protection officer. We increasingly see conflicts between local laws especially from countries outside the EU and the GDPR regulation itself. These conflicts mean that organizations are forced to make challenging decisions, sometimes with unknown legal consequences and hence consulting widely amongst experts in your organisation can be necessary to fully understand the potential risks.

Based on our client conversations we observe that there is some uncertainty around data productions which are to be made to authorities in countries not covered by GDPR and which may not have an adequate level of data security and protection. As many external regulatory driven investigations often involve US authorities, we assume most productions in countries not covered by GDPR are going to the US, but we do not have statistical evidence that this is necessarily the case. The GDPR law provides two exceptions to produce to such countries, namely Legal defence (Article 49 (e)) and Legitimate interest (Article 6 (f)). From previous experience producing under Legal defence requires companies not just to ensure that there is a legal case to produce the documents but also a necessity to test which information can be provided without redaction.

58% of respondents have not yet had to produce data to authorities in countries not covered by GDPR and which do not have an adequate level of data security protection. The challenge that can be faced is that requests from authorities are often received with challenging deadlines, however agreeing internally on how to respond and setting-up appropriate internal processes is time consuming. This can easily result in production delays, which in the context of the wider investigation can risk the ongoing relationship with the regulator and the benefits of “collaboration credits” in the overall resolution process. To overcome these challenges we suggest proactively discussing response plans & setting up teams to react quickly when required may be worth the investment of time upfront.

“I have always been very sympathetic to the principle that we should collect personal data for specified, explicit and legitimate purposes. It goes without saying that investigations data must be processed lawfully and fairly and be collected only for relevant purposes. I believe GDPR provides a solid framework to guide us”

Katie Hodson

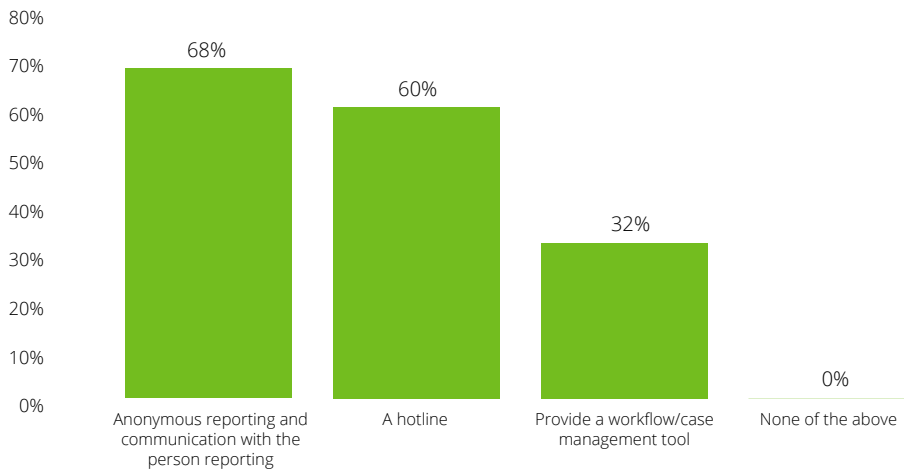
Head of Investigations
The Global Fund to Fight AIDS, Tuberculosis and Malaria

Speak Up Lines

The vast majority of organisations (over 80%) have a defined Speak Up line policy. 72% have a Speak Up Platform in place, of which half are managed internally and half externally.

The Speak Up platforms in use generally have features which allow for anonymous reporting and communication with the person coming forward, largely through the use of a hotline. Less frequently (for approximately a third of cases) the Speak Up platform provides a built-in workflow or case management tool.

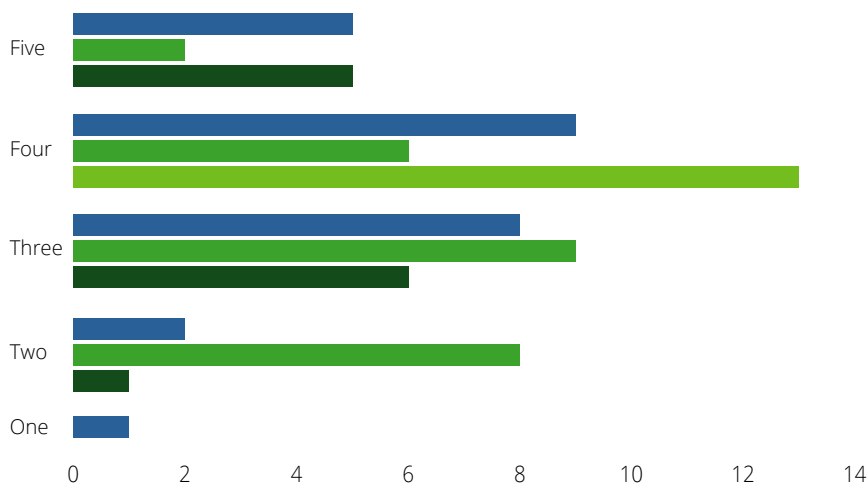
Does your Speak Up line platform include any of the following features



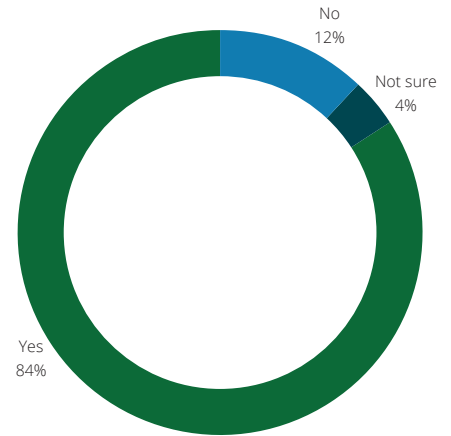
How confident are investigations functions that employees feel comfortable reporting issues via the Speak Up line?

The overwhelming majority of Speak Up line issues are managed by the investigation function, even if after initial triage by the external provider of the Speak Up platform, or by another internal department such as Compliance.

How confident are you that people within your organisation feel comfortable in 'speaking up' in respect to the following potential code of conduct violations?



Does your organisation have a defined Speak Up line policy?



"A speak up line platform should allow for communicating with anonymous reporters in a secure and confidential manner. I believe that maintaining confidentiality and providing anonymous reporting channels are crucial for a speak up culture. When looking at global substantiation rates, there is not a major difference between anonymous and named reports. In fact, the percentage of substantiated reports seems to be a bit higher for reports where the reporters remained anonymous."

Philipp Becker

Member of the Board
CeDIV - Cross-border eDiscovery,
Privacy & Investigations Association

Five = Most Confident
—
—
—
One = Least Confident

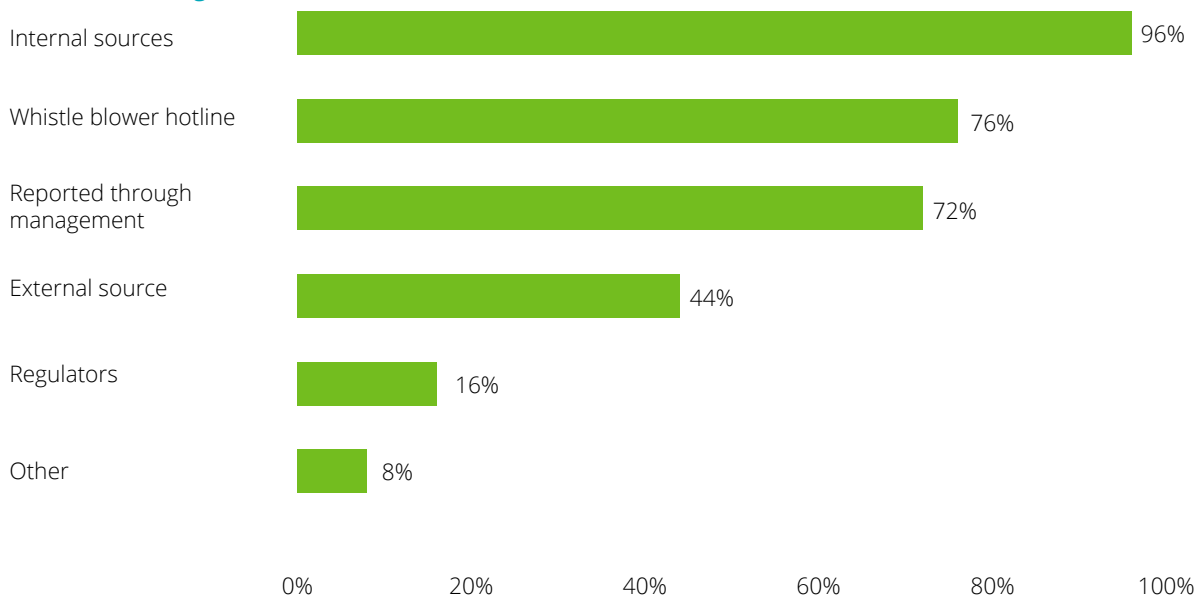
- Internally where they would need to report on actions of employees reporting to them/in a more junior role
- Internally where they would need to report on actions of peers or superiors
- Where the actions of an external party actions may impact on your organisation

There is some variation noted in the confidence which the investigation function has in whether employees would be comfortable to use the Speak Up line to report code of conduct violations, depending on who is implicated by their reporting.

Perhaps, understandably, there appears to be more confidence that employees would report on actions of external parties which may impact the organisation, however, when it comes to reporting on the actions of peers or superiors, there is less confidence that employees would feel comfortable doing so.

We note however, that there was not a strong indication that externally provided Speak Up lines elicited more confidence in employees using the line. This is somewhat surprising, but may suggest that the stronger influence on speaking up comes from the organisations wider culture and not the manner in which the Speak Up line is implemented.

Sources of investigations:



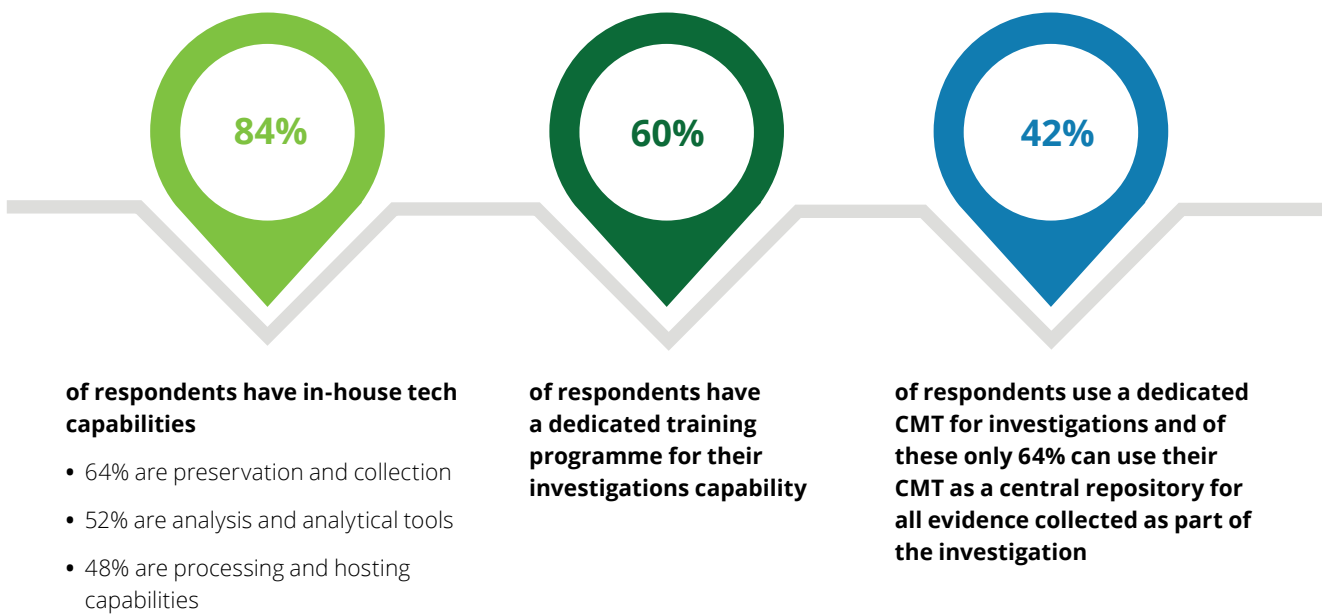
Nearly three quarters of respondents indicated that information provided via their Speak Up line was a source for investigations, with approximately two thirds of these indicating that information provided via their Speak Up line accounted for 50% or more of their investigations. Therefore, whilst the Speak Up line appears to be a key input for internal investigation teams, the data suggests that investigation teams are not wholly confident that employees will actually use the line.

This points to an opportunity for improvement in communication around the Speak Up line, encouraging employees to use the platforms provided and to provide assurances that information provided is acted upon and dealt with in a confidential manner. Potential communication channels which could be used include newsletters, e-mail, posters, intranet or internet posts, personnel meetings, town halls, training courses, internal bulletin boards or handheld flyers, brochures, wallet cards, social media, in person meetings or a combination thereof to suit the corporate culture of each individual organisation. Companies may need to adopt a flexible approach to encourage the use of a Speak Up line gauging the intake of reported issues, which can vary and may require reminders from time to time.

Technology and Data

It is hard to think of any part of a business which has not been impacted by the increasing amounts of available data and the use of technology to drive insights. This is also the case for investigation functions, which are now expected to access and analyse data from a myriad of sources. Having the in-house capabilities to access, process, manage and analyse data in an effective manner is critical, as investigations are increasingly technology and data led.

We note that 84% of respondents have in-house technology capabilities, with two thirds having preservation and collection skills, just less than half having processing and hosting capabilities and 52% having analytical tools.



Only 23% can cover all technological aspects of an investigation whilst 18% have no in house technological capabilities at all. Where an investigation function cannot cover a technological aspect they typically outsource this to a specialist provider, for example we note that 52% of respondents outsource their Forensic Technology or eDiscovery services and 28% outsource investigation needs related to Data Analytics.

- 64%** Preservation and collection
- 52%** Analysis and analytical tools
- 48%** Processing and hosting

Therefore using a provider with an established knowledge of your organisation can help to manage this trade off. Additionally, since data and technology are ever evolving, keeping up to date with latest tools and techniques may require significant investment in training staff and acquiring required software and therefore organisations can benefit from leveraging the skills of SMEs, outsourcing specific technological aspects.

Data landscapes

One area, which we see as an enabler for investigations functions, is to have a good understanding of your company's data landscape. So often we see investigations stall because there is a need to first undertake a process to understand what data is available, where it is stored, how access can be gained, who owns systems and can provide the required authorisations. This issue is especially prevalent in international organisations, with different systems operating in different locations, or where there are legacy systems arising from previous mergers and acquisitions. Maintaining an up to date understanding of the data landscape is critical to ensure all relevant data sources can be identified and accessed in an efficient manner. Data privacy considerations, which we expand on below, clearly need to be kept in mind when accessing and transferring any such data.

eDiscovery

40% of respondents use a Native file / email only review to conduct an electronic document review but 28% of respondents still perform a manual review of hard copy files (print outs) as part of the electronic document review in an investigation. It is somewhat surprising that email reviews are still conducted in hard copy. We note though, that for some in-house investigation teams, the majority of their time may be spent reviewing smaller cases where it would not be economical to perform a full eDiscovery exercise using latest technology when a short, targeted review will suffice, especially in cases that are for internal purposes only.

This is perhaps an area where we may see the impact of Covid-19 on investigation functions. Investigation teams have been required to work remotely with their technology support also operating remotely, therefore moving to an electronic review method may have been prioritised, and will continue to be the modus operandi post Covid-19.

CMT

We note that only 42% of respondents use a dedicated case management tool ("CMT") within their investigation function and a third of these cannot use their CMT as a central repository for all evidence collected as part of their investigation.

For those respondents who do use a CMT, it appears that they may not be using the CMT to its fullest potential, for example preventative and corrective actions are only recorded within the CMT by 50% of respondents, similarly only 36% share the case results as recorded in the CMT with other departments within the organisation. This is despite the fact that two thirds of respondents note that other departments, notably Compliance and Management, are responsible for ongoing monitoring and follow up actions stemming from investigations.

We believe that organisations could benefit from the use of a strong CMT which allows an investigation team to manage, prioritise and allocate investigation caseloads effectively as well as acting as a consistent document repository. Furthermore, a CMT can support the handover of monitoring processes between all relevant divisions such as risk, internal audit and compliance.

"The use of technological enablers were critical to investigators during the Covid-19 crises, as they not only made it possible but increased the assurance depth and augmented the scope of investigations. The main challenge was to select tools and train the teams in a very rushed pace. In a way, Covid-19 forced investigators to excel using new tools and acquiring new skills, and this evolution marked a point of no return."

Vanessa Nigro

Global Internal Audit
Investigations and ERM Director
Dufry International Ltd.



Training and Development

Only 40% of all respondents have a formal training programme for their investigators and of these a total of 76% do not believe or are unsure that the requisite training needs are being met.

The remaining 60% of respondents do not have a formal training programme for their investigators and among these, only 13% are confident that their training needs are being met.

It is clear from these statistics that training for investigators is an ongoing challenge for organisations, whether they have opted to provide some training internally or not, there is a lack of confidence in the training provided being sufficient.

This training challenge is further complicated due to the diverse mix of backgrounds, skills and experience within investigation functions and therefore there is a myriad of areas where appropriate training is required, for example covering

latest technological advances to keeping up with regulatory requirements. A one training fits all approach which may work in other departments does not apply here.

40%

Have a formal training programme for investigators

24%

Are confident or high confident that the requisite training needs are being met

48%

Are unsure if the requisite training needs are being met

28%

Are not confident that the requisite training needs are being met

“The results on training reflects discussions with my peers. Often companies struggle to find the right training offer for their staff if internally or they do not have the capacity to provide the needed expertise.

An investigation can be very complex, with legal, psychological, organizational, business related, technical aspects just to name some of them. Adequate training mitigates the risk of major failures and pitfalls as well as ensure the right attitude and behavior from an investigator. Another important element however, remains the experience of your staff.

A professional investigation carried out by a function that has the independence in the organization will have more credibility internally, and externally with regulators if required. It inspires trust in your value system and fosters belief in your framework in place; your values and demonstrates commitment that you live up to them and helps to create a speak up culture where employees feel empowered to speak up and are taken seriously.”

Sandra Middel

Head of Group Compliance
Clariant

Deloitte Forensic in Switzerland

The Swiss Deloitte Forensic team helps clients act quickly and confidently in the face of financial crime, regulatory concerns and actions, or sensitive internal investigations into fraud, corruption and other misconduct. The team consists of around 90 individuals in Switzerland, with access to a global network of over 4000 expert professionals who combine forensic accounting and investigative skills with leading edge technology and advanced data analytics techniques to offer innovative solutions to our clients' legal, regulatory and financial crime problems.

Our Services include:

- **Investigations and Remediation**, helping to act quickly and confidently in the face of economic crime, regulatory concerns and actions, or sensitive internal investigations into fraud, corruption and other misconduct.
- **Financial Crime Advisory**, helping to respond to Financial Crime with an effective and efficient task force comprised of industry experience, subject matter expertise and technology support.

- **Forensic Technology**, analysing large amounts of unstructured data yields an intelligent, state-of-the art approach to eDiscovery, Fraud Analytics, and Digital Forensic.
- **Disputes & Litigation Advisory**, working with organisations and their lawyers in judicial and alternative dispute resolution forums, across a range of jurisdictions.
- **Financial Crime Analytics**, deploying defensible and proven analytical techniques and approaches to leverage data to continually improve surveillance systems and processes.
- **Market Conduct and Trade Surveillance**, our assessment and enhancement services helping to respond to key industry challenges in the trade surveillance domain.



About

The Association of Corporate Investigators (ACI) is a non-profit association formed to meet the needs of the corporate investigations' community.

Vision

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

Mission

- Promote the highest ethical standards, including an ACI members code of conduct.
- Support the professional development of members, including accredited qualifications, training, cross-industry insights on corporate investigations programmes and access to a knowledge resource centre.
- Develop an accredited corporate investigator qualification.
- Bring together the corporate investigations community to share best practice.
- Actively promote diversity and inclusion across the corporate investigation community.

To join the ACI or learn more please visit www.my-aci.com or contact us at admin@my-aci.com.

Contacts



Steve Young, CEO of the ACI

Steve served 20 years in UK law enforcement investigating economic crime specialising in the pro-active investigation of Banking Fraud, Bribery & Corruption, Whistleblowing and Money Laundering. This was followed by 6 years at Citigroup Inc. as EMEA Regional Director of Investigations, and 8 years as Barclays Bank Plc, Global Head of Investigations for Investment Banking & Wealth Management. Currently Head of Fraud & Investigations in Group Compliance at Lombard Odier, based in Geneva. To date, 40 years of international economic crime experience in both a law enforcement and corporate environment.

steve.young@my-aci.com



Katie Hodson, CAO of the ACI

Katie is the Head of Investigations, at the Global Fund's Office of the Inspector General. The Global Fund to Fight AIDS, Tuberculosis and Malaria is an international financing organisation that aims to "attract and disburse additional resources to prevent and treat HIV and AIDS, tuberculosis and malaria. Katie is from England and has more than 20 years of experience in conducting and supervising investigations. Prior to working at The Global Fund, she served at Novartis International AG, Basel as the Global Head of Investigations, where she managed a team of 30 investigators working on international matters. She has extensive experience leading fraud investigations globally, including product theft, diversion and counterfeiting as well as numerous investigations involving employee misconduct.

Katie.hodson@my-aci.com



Nic Carrington - Partner, Financial Advisory Zurich

Nic is a Partner in Deloitte's Financial Advisory practice in Switzerland. He specializes in forensic advisory, financial crime fraud and corruption investigations, advising on cases involving white-collar crime and corruption, including FCPA-related matters, anti-money laundering compliance and investigations, procurement fraud, conflicts of interest issues and accounting irregularities. Nic is a Qualified Accountant and a Certified Fraud Examiner.

+41 58 279 7146

nicarrington@deloitte.ch



Karen Williamson - Director, Financial Advisory Zurich

Karen is a Director in Deloitte's Financial Advisory practice in Switzerland. She has spent more than 13 years' working in Forensics and specialises in investigations, predominantly focussed on the Financial Services industry, including spending one year on secondment to the Financial Services regulator in the UK, the FCA.

Karen is a highly experienced Forensic accountant and investigator and has worked in the UK, Germany, China and Switzerland on a wide variety of investigations. Advising clients and liaising with external counsel on matters ranging from fraud and misconduct investigations; insider dealing; allegations of conflicts of interest; bribery and corruption investigations; to panama papers exposure analysis; tax evasion; accounting investigations; and employee expenses fraud.

+41 58 279 6331

kjwilliamson@deloitte.ch



This publication has been written in general terms and we recommend that you consult a professional before acting or refraining from acting based exclusively on the contents of this publication. Deloitte AG disclaims any duty of care or liability for losses suffered by anyone who acts or fails to act as a result of the contents of this publication.

Deloitte AG is a subsidiary of Deloitte NSE LLP, an affiliate of Deloitte Touche Tohmatsu Limited ('DTTL'), a UK private company limited by guarantee. DTTL and its network of affiliate companies each form an independent and separate legal entity. DTTL and Deloitte NSE LLP do not provide services to clients. For a detailed description of the legal structure of DTTL and its related companies, please consult www.deloitte.com/ch/about.

Deloitte AG is an audit firm recognised and supervised by the Federal Audit Oversight Authority (FAOA) and the Swiss Financial Market Supervisory Authority (FINMA).

© 2021 Deloitte AG. All rights reserved.

Designed by CoRe Creative Services. RITM0686251