Deloitte.

Considerations for undertaking fraud and misconduct investigations remotely

May 2020 | For private circulation only

Introduction

The disruption brought about by the COVID-19 pandemic has forced us to rethink our business processes and relook at how we perform certain activities. As days go by, it is becoming clear that things will not resume normalcy in one go. While the lockdown may slowly be removed, precautions will continue and remote working in some form may remain 'the new normal'.

In the current environment, internal investigation teams are facing more pressure due to realigned business priorities, changes in business operations, and cost considerations. It is not uncommon for past incidents of fraud and misconduct to surface during a downturn and new fraud instances to emerge (as a result of performance pressure on businesses and individuals). Thus, the workload of internal investigation teams is likely to increase.

How prepared are internal investigation teams to tackle fraud in this new environment? While assessing new fraud risks and putting in place added controls is one aspect, preparing appropriate response protocols and procedures to deal with an incident/allegation is also important. This document explores some key challenges that investigation professionals may encounter in the current scenario and suggests some considerations to deal with these circumstances.

Current state of business

Factors affecting corporate fraud investigations

Remote and scattered presence of individuals involved, including the following:

- Investigators
- Key stakeholders, including management and process owners
- Witnesses and sources
- Suspects/respondents

Limited/restricted physical access to the following:

- Office premises and infrastructure
- Data and documentation
- Computer devices used by suspects/respondents and other technological artefacts
- Business premises of third parties alleged/suspected to be complicit/aware of the ongoing matter under investigation

Cost restrictions on account of lower revenues leading to the following:

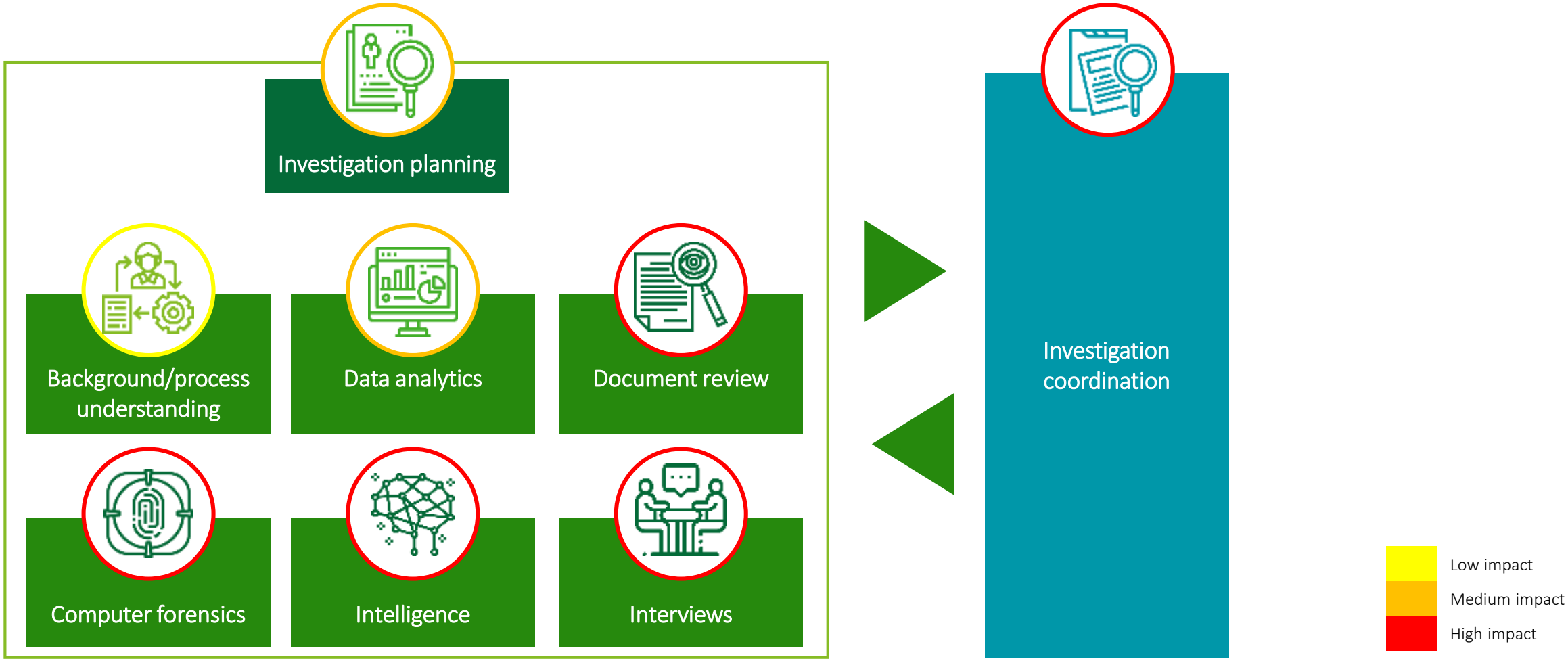
- Modified budget/spending priorities
- Prioritisation of critical matters/allegations for investigation (regulatory/law-enforcement matters, senior management misconduct, brand/reputational matters, matters of significant financial impact, schemes emerging as a result of the pandemic situation, etc.) and deferring of non-critical matters

The current economic/business environment leading to increased fraud vulnerabilities and ensuing investigations in certain areas, including the following:

- Financial statement fraud
- Insider trading
- Misappropriation of funds/assets
- Data breaches

Typical corporate fraud investigation process

Procedures/activities likely to be affected



Investigation planning

Some considerations

- Is physical access to data sources/documentation required? How can investigators manage without such physical access?
- Can large datasets be transferred to the engagement team over a secure email or portal? What are the secure file sharing options available for such data transfers?
- Are computer forensic procedures required as part of the investigation? How much data can be obtained from the server/cloud storage? How will the imaging of laptops/desktops/mobile phones be undertaken?
- How will interviews be undertaken? What are the options if interviews cannot be conducted in person? What is the best approach to conduct interviews over a videoconference? What could go wrong and how can such issues be addressed?
- What steps need to be taken to ensure that despite a scattered physical presence, the investigation team is aligned to effectively manage work procedures and use new information discovered from each work stream appropriately across the investigation procedures?

Background and process management – Some considerations

Background/process understanding

Discussions

- Background discussions and informational interviews for process understanding may be undertaken over a call or video meeting.
- Pre-read of allegations, SOPs, relevant policies, and process documents may be necessary to optimise efficacy of discussions.
- In the absence of detailed background information and limited policy documents, investigators may circulate a questionnaire seeking responses from stakeholders on select aspects pertaining to the case. This may be followed up with a discussion for clarifications.

System/transaction walkthroughs

- Concerned stakeholders may run system walkthroughs over an online meeting with screen sharing.
- Control may be shared with investigators to explore tool functionalities as required.

Process walkthroughs

- Physical visits to shop floor/warehouses and business establishments may be curtailed in line with current operating circumstances.
- Such a situation may be managed by (a) reading defined process flows, (b) process videos/live beaming the process and (c) discussions (audio/video) with concerned process/activity owners (discussions with activity owners may need to be more detailed/pointed given the physical limitations in examining the process).

Data gathering and analysis – Some considerations

Data analytics

Data access

- Use remote access to the ERP to download the data, depending on the systems under use and data size.
- Ensure security of the remote access connection

Data transfer

- Transfer the downloaded data (whether by remote access or directly by an individual with appropriate access rights) to relevant members of the investigation team over a secure data sharing site.
- Data shared over email may be encrypted/protected.
- Avoid sharing data to public domain IDs/personal email addresses.

Analyses and results

- Clear allocation of work in terms of data processing and analyses to eliminate the possibility of duplication of work
- Real-time sharing of results (after review, checking for false positives, etc.) with other members of the investigation team for discussions and consideration in other work procedures to be done with a collaboration tool (MS Teams, etc.)

Data sanctity

- Ensure that the data provided was appropriately extracted from the system (including completeness of relevant data fields, period, no unwarranted filters, etc.).
- A stakeholder can extract the data with the investigation team joining over video conference or screen share to observe and validate the process followed and thereafter transfer the correct dataset over secure file sharing options.

Ensuring adequate infrastructure including a strong and secure network and secure data sharing platforms is critical to carrying out these activities remotely.

Transaction testing/document review – Some considerations

Document review

Soft copy documentation

- Where soft copy documentation is uploaded to the ERP/relevant system as part of standard process, it may be retrieved over remote access to the network.
- Relevant stakeholders may scan and share the soft copy via a secure reading room or official email over a safe network and in encrypted form if needed..
- For scanned documents reviewed, if forming part of the investigation evidence (and especially in case of litigation), access to and preservation of the original physical document may be essential and should be planned for.

Hard copy documentation

- Investigations usually require access to some extent of physical documentation.
- Organisations should restrict employees carrying physical documentation home where possible: hard copies should be retained in the office/document storage for ease of access/retrieval.
- Carrying hard copies home may compromise security of documents. Further retrieval of documents will require a notification to and cooperation of the concerned employee.
- Organisations may increasingly shift to electronic documentation given remote working considerations.

Computer forensics | Collection and review – Some considerations

01

Enterprise/cloud data sources

Secure retrieval of server data/data stored on the cloud should remain largely unaffected as this can be accessed and downloaded over the network with support from the IT team, and transferred to the investigation teams over an SFTP/secure file sharing platform.

02

Enterprise collection software

For organisations using enterprise collection tools, copying data from custodian devices remotely over the company network may be possible with the support of the designated team/IT. However, while doing so it must be ensured data is not tampered and the chain of custody is intact. Organisations may deploy enterprise collection tools in the future to enable data retrieval from devices at remote locations, provided there is adequate network strength and security to undertake this activity.

03

Encrypted hard drive with preloaded scripts

With limitations in physical device collection for evidence gathering, investigators may consider the option of gathering data from custodian devices via an encrypted hard drive (preloaded with scripts to run the imaging) that can be connected to the device and initiated by the custodian. However, this may be possible only for open investigations where the custodian is aware of the proceedings and is cooperative in securing data. Data destruction attempts are a possibility.

Notes

- Securing physical access to image devices would require custodian notification: consider during investigation planning. For example, check the availability of backups/datasets that can be secured from other sources before notifying custodians to better preserve evidence.
- Reviewing company policies and protocols regarding work from home (e.g., using the official network through VPN rather than using open networks) and regarding rights to secure data from physical devices used for official purposes (as required by the company), may be necessary.
- DLP logs may be reviewed to monitor/report possible unauthorised deletion of data transfer through online modes or USB ports (assessing the effectiveness of the DLP mechanism may be necessary). Organisations may need to reassess their DLP systems and adequacy of logs.
- Using an eDiscovery platform to manage and review digital evidence can help in the centralised tracking and control of review progress and status, comments, and prepare for data to be produced as evidence in a court.
- Organisations may have data privacy considerations for allowing 'bring your own device' (BYOD) for remote working: possible challenges in collection/review of data from such devices as a result of data privacy concerns may need to be assessed and addressed in organisational policies.

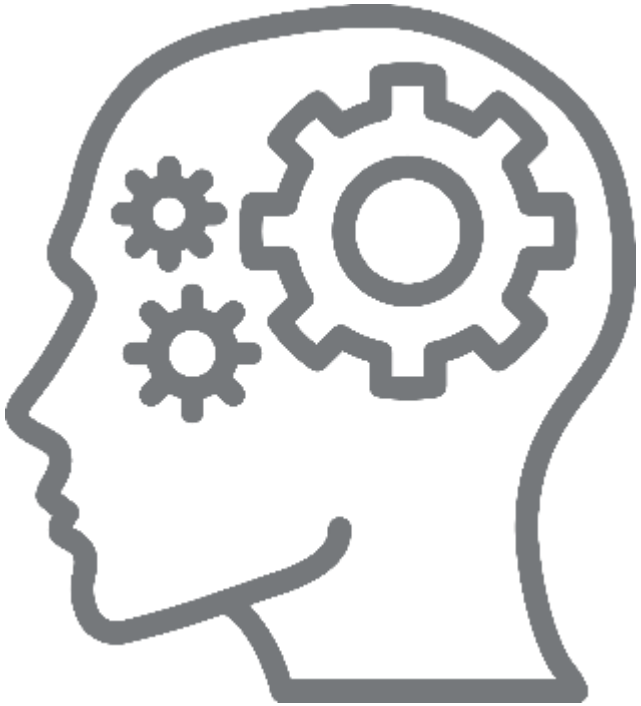
Intelligence gathering – Some considerations

Intelligence

L1

Corporate filings, litigation databases, creditworthiness checks, regulatory checks (bankruptcy/insolvency, international watch lists, etc.) continue as usual to the extent available online

Public domain searches, adverse media, social media mapping, to remain largely unaffected



L2

Validating existence of entity/business, key individuals, business relationship mapping, etc., may largely be done over call and from online sources.

Due to restrictions in physical movement, it may be challenging to undertake site verification of the entity or assessing operational aspects via in-person source enquiries

Interviews

Considerations for remote interviews

Interview sequence and protocol

- Planning around interview sequence and timing may be required where there are multiple targets to prevent information sharing in-between interviews.
- Standard interview process/protocols will be followed that includes setting the context, discussing applicable policies under which the interview/investigation is being conducted, allowing the interviewee comfort breaks, and 'support person' if the policy allows.

Environment

- One of the biggest challenges of a remote interview is limited control over the interview environment and interviewee. Ensuring an appropriate environment, including a quiet place, and the ability to speak confidentially for both the parties , is important for an interview for both the parties.

Recording

- Legal considerations are to be kept in mind and complied with while recording an interview, for e.g. seeking the interviewee's consent on the record where required.
- Irrespective of whether the interviewee informs the interviewer of an intention to record, the interviewer may place on record that they do not consent to be recorded. However, they need to be mindful that interviewees may covertly record the conversation

Mode

- In-person interviews are always preferred. If not possible, a video interview is preferred over an audio interview.
- A video interview enables the interviewer to observe the interviewee's expressions and body language, the environment, presence of other individuals, etc.
- Irrespective of the mode of interview, do consider that respondents who are reluctant to cooperate could use the remote interview setting to their advantage.

Infrastructure

- For a video/audio interview, having a reliable/strong and secure connection at both the ends is imperative.
- Consider dealing with a power outage: what will be affected and how will it be managed? Is power backup available at both the ends?
- Advance testing is recommended to ensure a seamless meeting.

Document sharing

- Consider sensitivities/risks of sharing documents with the interviewee beforehand or during the interview (controlling circulation).
- Documents may be presented during a video meeting or shared using a secure data room with read-only access to the interviewee during the course of the interview (consider that the interviewee may still be able to take screenshot or photo of documents).

Other general considerations

Case management
Case management tools may help effectively document and track investigation progress, and maintain an audit trail for case updates, report edits, etc.

Collaboration tools
Using collaboration tools (e.g., MS Teams) may help streamline execution and collaboration between work streams, prevent duplication of work, and help the investigation team stay aligned and updated on recent developments/observations from other work streams..

Confidentiality
Reinforce confidentiality within the investigation team and in their interactions with other personnel as part of the investigation. For example, taking calls privately, avoid using speakerphones, not leaving case documents unattended at home, following document printing considerations, using secure file transfer/sharing platforms, etc.

Prioritisation
Since the downturn environment is known to increase pressure to commit fraud, reported instances of alleged fraud may increase. Constrained budgets may be a challenge and prioritising matters for immediate investigation may be necessary.

Standard protocol
Consider that the standard investigation protocols will still need to be followed, including maintaining chain of custody, following due process, evidence collection and preservation, and stakeholder management. Limitations due to the pandemic cannot compromise the integrity of the investigation.

Report writing
Investigators need to plan for integrating observations from different (scattered) work streams and team members effectively to join the dots and draw out observations from a 'big picture' perspective. They also need to delegate responsibility for writing each section of the report to team members. Further, data storage options must be considered to share working copies of the report.

Conclusive Remarks

Corporate fraud investigations do not have to be stalled due to the COVID-19 crisis. Delays in the investigation process can significantly alter outcomes and provide favourable conditions for fraudsters and involved parties to tamper evidence and get-off scot free. When organisations are struggling to survive, undetected fraud can further dent their ability to perform effectively in a tough environment. While many organisations are discussing the need for strong internal controls, equipping internal investigation teams to continue their work is equally important.

Key contacts

Nikhil Bedi
Partner and Leader
Forensic – Financial Advisory
nikhilbedi@deloitte.com

Kavita Nathaniel
Director
Forensic – Financial Advisory
knathaniel@deloitte.com

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

This material is prepared by Deloitte Touche Tohmatsu India LLP (DTTILLP). This material (including any information contained in it) is intended to provide general information on a particular subject(s) and is not an exhaustive treatment of such subject(s) or a substitute to obtaining professional services or advice. This material may contain information sourced from publicly available information or other third party sources. DTTILLP does not independently verify any such sources and is not responsible for any loss whatsoever caused due to reliance placed on information sourced from such sources. None of DTTILLP, Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this material, rendering any kind of investment, legal or other professional advice or services. You should seek specific advice of the relevant professional(s) for these kind of services. This material or information is not intended to be relied upon as the sole basis for any decision which may affect you or your business. Before making any decision or taking any action that might affect your personal finances or business, you should consult a qualified professional adviser.

No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person or entity by reason of access to, use of or reliance on, this material. By using this material or any information contained in it, the user accepts this entire notice and terms of use.