Baker McKenzie.

5 LUNAR NEW YEAR'S RESOLUTIONS FOR INVESTIGATIONS

About Baker McKenzie's Investigations, Compliance and Ethics Group.

Our Global Investigations, Compliance & Ethics Group of 500+ lawyers across 74 offices provides compliance risk advice and conducts internal and regulator-driven investigations in a variety of areas: anti-bribery and corruption, anti-money laundering, whistleblower complaints, sanctions and boycotts, anti-trust, data privacy, cybersecurity, fraud, tax, regulatory conformance and enforcement and HR misconduct. We assist multinational clients with internal and external cross-border investigations. We understand national regulatory processes, legal powers, and enforcement tactics used in taking enforcement actions. Please do reach out if you would like to discuss further.

As we say farewell to the Year of the Rabbit and move into the Year of the Dragon, it is a good time to reflect on the challenges faced, your successes, and what lessons you have learned along the way.

It is also a good time to set yourself some goals and resolutions. To help you on your way, we are pleased to share our top **5 Lunar New Year Resolutions** for handling **Internal** or **Government Investigations:**

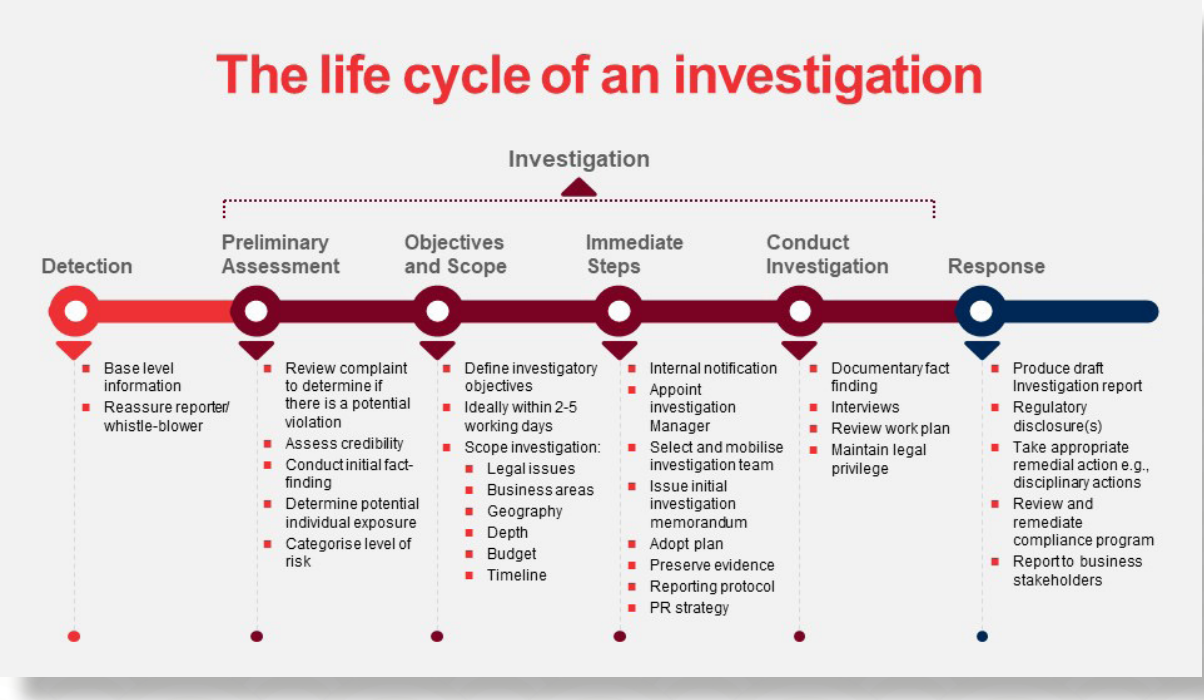
1. **I will prepare an investigation plan.**
2. **I will take care collecting and reviewing data.**
3. **I will preserve legal professional privilege.**
4. **I will prepare my team to prevent a crisis.**
5. **I will make sure that the problems we find are fixed.**

Investigations are an essential tool for ensuring a company's ethical standards are being followed by employees, business partners, and any others with whom the company interacts. However, investigations are also an essential tool for demonstrating and maintaining strong corporate governance – an integral part of a company's ESG commitments and strategy.

I will prepare an investigation plan.

Well begun is half done

Once an investigation is triggered, whether by a whistleblowing complaint, an internal audit or an inquiry from a regulatory authority, business leaders want an outcome as soon as possible. However, it is important to pause to properly plan and scope the investigation – prepare a written investigation plan with clear and concise objectives and scope, as well as the anticipated steps from start to finish, so you have a blueprint to follow. Memories of how urgent the matter was at the outset will fade over time, but a well-crafted plan will guide your way and record the path taken.



The primary purpose of the plan is to keep the investigation focused and structured. With a clearly identified scope in mind, you will be able to focus on the identified issues and work through the steps in a structured manner and within the timeline you set. It will also help when it is time to prepare your findings of fact and recommendations – you can refer to the plan to ensure that the deliverables are in clear if not parallel structure to the issues identified, and that nothing has been overlooked.

Failing to plan is planning to fail

Failing to properly plan and scope the investigation comes with the risk of having an unreasonably wide or expanding scope without focusing the key issues. Without a plan, it will be difficult to recognise if the investigation veers off-track, which can result in wasted effort, time and cost. It may even prevent you reaching the "finishing line" if there are issues left unaddressed.

Lack of planning may also lead to these common mistakes:

Failing to consider at the outset whether the investigation can be protected by legal professional privilege. Having legal counsel involved at the start of the investigation not only allows for continuous assessment of potential liability, strategic direction and disclosure obligations, but also can protect the investigation itself from potential disclosure.

Dismissing the importance of data review. Where a large amount of data may be involved, preservation at the outset is key. A common misconception is that all of the data must be reviewed, or none at all. Reviewing the right data at the right time, using AI tools and considering data privacy and other legal risks is fundamental and will not only manage the costs, timeline and resources, but also allow for the investigation to pivot in direction if needed.

Involving stakeholders in the investigation team. The team should be independent to protect the investigation from actual or perceived interference or conflicts. This does not mean that other stakeholders should not be kept informed – they will ultimately be the ones who will need to make decisions. However, an independent investigation will be more credible and defensible, which is not only something that is considered by external authorities and regulators, but also an important part of good corporate governance.

Best practices for investigation planning

So what should you consider when formulating your investigation plan?

01

What is the preliminary assessment?

You should first consider if there is anything that must immediately be dealt with – is there a violation of law or regulations, or does anything need to be stopped or reported or personnel to be protected? Where there is a whistleblower or complainant involved, you should of course assess the credibility of the report. However, desist from taking steps to identify the whistleblower or otherwise prevent the whistleblower from reporting to regulators or other authorities – this may expose the company to additional penalties.

02

What are your objectives and scope?

This requires "triage" where you determine what factual issues need to be resolved and what steps will be required to resolve them. You will also need to consider whether other business divisions or functions may be impacted, which jurisdictions might be involved and the potential areas of legal or other risks. All of these factors will allow you to formulate a clear scope, clarify the steps you will take, and determine the likely timeline.

03

How will the investigation be conducted?

The make-up of the investigation team is crucial – and they will need help from legal, compliance, HR, IT, finance, audit and corporate communications, as well as external sources such as law firms or forensic accountants. As mentioned above, make sure the team is not conflicted in carrying out an independent investigation, to maintain the credibility of the findings and with the protection of legal professional privilege.

I will take care collecting and reviewing data.

The collection and review of evidence – witnesses, documents, photos, voicemails – informs your investigation findings.

How should you deal with the electronic data?

In this digital age, most investigations require the collection and review of electronic data. This will come from a number of sources, including emails and shared drives, but also from phones and laptops. This data can be easily collected, duplicated, and transferred to multiple teams – such as in-house investigators, external legal counsel, and forensic accountants – at the click of a button. However, data needs to be handled carefully, given the patchwork of legal restrictions on transferring personal data around the world. Moving and transferring data across jurisdictions increases the risk that you may inadvertently breach these laws.

Make sure to review the restrictions on data transfer that may apply

Common restrictions are:

Personal data privacy The overarching principle in some jurisdictions is that informed consent must be obtained before personal data can be transferred to a third party or used for a purpose not initially disclosed to the data subject. There are often additional requirements where personal data is to be transferred outside of the country (even if within the same corporate group), such as the PRC's Personal Information Protection Law (PIPL). Some data protection regimes – such as the EU's General Data Protection Regulation (GDPR) – even have broad extraterritorial application, so multiple rules may apply at the same time.

National security / state secrets legislation can cover any data which may impact national security and state interests such as state policy and decision-making, data of state-owned enterprises, or even statistics about key state-sponsored industries (e.g., energy, technology, national defence). Depending on the nature of the data, you may require government approval or be subject to a blanket transfer prohibition.

Blocking statutes may be triggered where the data is for disclosure to foreign authorities or used in foreign court proceedings. This can lead to a "Catch-22" situation where foreign authority or court orders disclosure, but at the same time the disclosure is prohibited by home legislation.

So what can you do?

1 Make sure your data is preserved

Ensure that all data that might be potentially relevant to the allegations under investigation is preserved, by turning off the auto-delete function on email accounts or taking a back-up of the server.

2 Carefully scope the data collection and review

Instead of imaging everything, try narrowing the dataset for collection and review using carefully scoped search terms and/or limiting the review to certain folders or drives.

3 Control the recipient list

Sensitive data should be shared on a need-to-know basis and protected by other controls e.g., encryption, multifactor authentication, password protection.

4 Take care when dealing with national security / state secrets

Certain clients (e.g., state-owned enterprises) or industries (e.g., energy and technology) pose higher risks. You need a legitimate objective for launching the investigation that does not infringe national interests. Data must be well protected and not be dealt with in a way that can be viewed as endangering national security (e.g., sharing it with sensitive or conflicting parties in a foreign country).

5 Localize the investigation

Consider conducting the investigation entirely in-house or with internal and external teams within the same country. If data has to be transferred out, restrictions should be assessed on a country by country basis. For example, data transfers from an EU country to New Zealand are less restrictive than transfers from an EU country to Australia.

6 Seek assistance from foreign / home authorities

You can consider asking the foreign authority or court to obtain the data through judicial cooperation routes (e.g., mutual legal assistance treaties) or seek a waiver of data transfer restrictions from the authority.

7 Manage the data created in the investigation

Data transfer restrictions do not just apply to the initial extraction and transfer - any communications or work product with extracts of the data also needs protection.

3 I will preserve legal professional privilege.

What's the deal with privilege anyway?

Broadly speaking, common law jurisdictions such as Hong Kong, Singapore, Malaysia and India retain the common law concept of legal privilege, which comprises **legal advice privilege** (the protection of confidential communications between clients and their lawyers made for the dominant purpose of legal advice), and **litigation privilege** (protection of confidential communications created for the dominant purpose of use in actual or contemplated litigation).

US privilege also includes a "work product" doctrine which extends over documents prepared by an attorney "in anticipation of litigation"; the materials need not be communicated to the client to receive protection.

In civil law jurisdictions, while there is usually no formal concept of "privilege", certain confidentiality protections are afforded under attorneys' professional secrecy obligation (e.g., the PRC).

What happens if privilege is not protected?

When you commence an investigation of issues identified such as through a whistle blower report or employee complaint, it often falls to the internal audit team, HR and/or in-house counsel to undertake the investigation.

If there has been little to no involvement by legal counsel in the investigation process, interview memos, reports and any relevant communications may not attract legal professional privilege. Without privilege, these documents may need to be handed over to third parties if requested, including regulators and law enforcement agencies (both local and abroad) or in litigation proceedings such as employee disputes. Privilege provides more control in your hands as to when, if, how and with whom, investigation findings are shared.

So how do I protect privilege in a multi-jurisdictional investigation?

- Consider which jurisdiction presents the greatest risk if privilege is lost. Structure management of an investigation in a jurisdiction with robust privilege protections.
- Have legal counsel run the investigation. If in-house counsel are not "on the ground", engage external counsel.
- In-house counsel often wear many hats. Privilege may be challenged if the lawyer is in fact acting in an administrative or business capacity. Some countries such as India and Malaysia do not recognize privilege for in-house lawyers.
- Limit the creation and circulation of documents. Where sensitive information or legal advice needs to be in writing, it should be limited to communications between lawyers and their client. These documents should not be distributed to the business.
- Establish a communications protocol and use a web-based tool for document review.

Are my interview notes protected by privilege?

- Interviews should be conducted by internal or external counsel. It should be made clear to the employee that the investigation is to remain confidential and when external counsel conducts the interview, it must be made clear that the lawyer is engaged by the company and not any specific individual.
- Any interview notes should include counsel's thoughts and impressions and not just a verbatim record.
- Interview notes should state that they contain legal advice and, if appropriate, that it has been prepared in connection with anticipated, pending or threatened adversarial proceedings.

What about my communications with third parties such as auditors and regulators?

- Be aware that disclosures of information to regulators, auditors or shareholders could waive privilege over the investigation. Providing high-level summaries or facts can strike a balance between providing necessary information and safeguarding privilege.
- Use express terms in disclosures stating that:
  - Documents and information are provided on a strictly confidential basis and for the sole and limited purpose of the current inquiry (and not for any other potential or contemplated regulatory investigations or proceedings).
  - The third party will not disclose any of the materials to any other parties without written consent.
  - Privilege is claimed over the materials provided, including under any applicable statutes.
- There are benefits in conducting a robust internal investigation in the context of obtaining cooperation credit from regulators. French prosecutors recently recognized the "relevance of internal investigations" as a mitigating factor which reduced the size of the fines imposed against companies. However, providing information in one jurisdiction may result in publication of information in another; where disclosure must be made in one jurisdiction, consider whether disclosure should be made in ALL jurisdictions.

I will prepare my team to prevent a crisis.

Expect the Unexpected

There are many events that can turn into a crisis – cyber incidents, media reports, regulatory action and dawn raids. While you may not be able to predict when these happen, you can prepare your team on how best to manage them with control and calm. This is particularly important for dawn raids and other unannounced visits by regulatory or government authorities, but the below general principles can be applied across the board, including cyber incidents.

Plan for a Dawn Raid

The first step is to develop a dawn raid protocol.

This protocol should contain easy-to-follow steps and procedures, starting with the moment the officer walks through the door and ending with what you need to do after they leave. It should also include guidance on communications – bearing in mind that you may be bound by secrecy obligations around most government investigations and enforcement action. As more companies are adopting remote or hybrid working model, the protocol should also be updated to address potential dawn raids at homes which could be daunting for employees and their family members.

Next, make sure to explain and train all company personnel – including directors, employees, secondees and contractors – on the protocol and the steps to be followed.

Trainings should be customized to ensure that the relevant functions, especially the front-line staff (usually reception or security), IT, facilities management and legal teams who will be dealing with the authorities are familiar with their respective roles, rights and obligations during a dawn raid. You should make sure your employees are aware of how to deal with authorities or regulators, should they turn up at home. You may even consider conducting a mock dawn raid to identify any weaknesses in the protocol and allow the employees to practice their response.

Designate a raid response team

This is a special team of employees and external professionals to prepare for and respond to a dawn raid. Their contact details should be readily available at the front-line for instant response and assistance. The team members should collectively possess a the knowledge and expertise to enable them to respond to business, finance, legal, compliance and IT issues. Baker McKenzie's Global Dawn Raid App (available here), provides practical assistance and peace of mind for in-house legal teams and individuals handling unannounced inspections.

Dos and don'ts during the dawn raid

Dos

- Do remain polite at all times.
- Do follow your dawn raid protocol.
- Do check authority/ identification of the officers.
- Do prioritise the raid over your other work.
- Do co-operate fully with officers.
- Do allow officers access to your office and files.
- Do make sure to have a post-raid wrap up session to confirm what happens next.

Don'ts

- Don't panic.
- Don't obstruct the investigation.
- Don't delete, shred or remove files or emails.
- Don't volunteer extra information/documents.
- Don't communicate with others about the investigation.
- Don't talk to the media. Do not use Facebook/other social media.
- Don't sign anything unless you have approval from the raid response team.
- Don't break seals put on doors or cabinets by the officers.

Communications and reputation management

There are usually strict secrecy obligations when it comes to dawn raids and enforcement actions. During and following a dawn raid, employees should maintain confidentiality and refrain from communicating, discussing or sharing with anyone internally or externally about the visit.

However, there will be times when external communications are necessary, for example if the authority issues a press release or the matter otherwise becomes public. For these circumstances, you should have in place a plan for what happens next, such as whether to issue a press release and designating a media spokesperson. External assistance from legal and PR firms is highly recommended.

I will make sure that the problems we find are fixed.

I will move forward instead of simply moving on

Completing an investigation – particularly if it involves a serious legal or reputational issue – can be stressful given the pressure to get to the bottom of the issue quickly from a number of directions – management, employees involved, and other stakeholders. However, when you have your findings, it is important to make sure the company moves forward instead of simply moving on. This is where an effective remediation plan comes into play.

I will take appropriate disciplinary actions

One of the most frequent questions an investigator will hear from stakeholders is – can we just get rid of the problematic employee? In their view, this can be the most efficient and effective way of eliminating a problem, if in fact a problem does exist, without having to go through the time and effort of conducting an investigation. However, this approach can raise a number of legal and morale issues, and is not a good example of proper corporate governance practices.

If your findings of fact conclude that there has been some wrongdoing, then disciplinary action may be appropriate. Not only will it remove the wrongdoer from the company, but it will also reinforce the message that the company takes misconduct seriously and will assist to deter future misconduct by others. The disciplinary process will generally be managed by HR teams to ensure that such actions are applied consistently and fairly. The specific employment consequences may be mandated by local laws or by employment terms, whether in agreements, regulations, work rules, or policies. To mitigate employee claims, it will be important to follow any required timeframe and complete any required steps leading up to the final disciplinary action (e.g., notice, disciplinary hearing and appeal mechanism). The disciplinary process, the basis of the disciplinary action and the final action enforced should be clearly documented and separate from the investigation report. These steps will be helpful if the company has to answer questions or claims about the disciplinary action taken.

I will review and implement/enhance processes and controls

In addition to any disciplinary action, you should also consider what processes and controls require enhancements or implementation, to reduce the risk that the misconduct recurs. For example, do you need more transparency over interactions with third parties? Or should you lower the approved gifts and hospitality thresholds? Do the staff involved need more regular training? Reviewing and refreshing your compliance program is a necessary part of good corporate governance and a necessary step to take following any investigation. While compliance issues crop up in all companies from time-to-time, the critical factor for regulators and enforcement authorities is how you respond to the issues.

I will conduct ongoing monitoring and ensure proper governance

After you have enhanced your processes and controls, it is important to make sure they are properly implemented and communicated. The tone must come from the top – leadership needs to support, resource and engage with the compliance program. This is key to demonstrating good corporate governance. The program should also be monitored regularly, by way of audits, to make sure it is working.

Whistleblowing or speak up programs are also a good metric for determining whether a company and its staff are embracing a compliant culture. If staff or third parties feel comfortable to raise issues through these channels, it demonstrates both an awareness of behavioural expectations, as well as confidence that the company will do the right thing. The lack of reports received either organically or through a whistleblowing process can be an indication of a poor compliance culture.

For more information on the hallmarks of a good compliance program, please check out Baker's 5 Essential Elements of a Good Compliance Program.

We recognise that navigating through an investigation can be a challenging task and properly executing a remediation plan is even more so. It requires continuous efforts to ensure that steps are taken to address the identified and potential issues.

We hope that our recommendations serve as a useful guide on your journey to promote strong corporate governance amidst any challenges encountered in the Year of the Dragon.

Our Team

Mini vandePol
Partner, Hong Kong
Investigations, Compliance & Ethics
+852 2846 2562
mini.vandepol@bakermckenzie.com

Henry Chen
FenXun Partner, Shanghai
Investigations, Compliance & Ethics
+86 21 6105 8521
henry.chen@bakermckenziefenxun.com

Christine Cuthbert
Special Counsel, Hong Kong
Investigations, Compliance & Ethics
+852 2846 1814
christine.cuthbert@bakermckenzie.com

Gerald Lam
Senior Associate, Hong Kong
Investigations, Compliance & Ethics
+852 2846 2138
gerald.lam@bakermckenzie.com

Karen Man
Partner, Hong Kong
Financial Services
+852 2846 1004
karen.man@bakermckenzie.com

Grace Fung
Partner, Hong Kong
Financial Services
+852 2846 2459
grace.fung@bakermckenzie.com

Jay Ruan
FenXun Partner, Shanghai
M&A
+86 21 6105 8577
zhenyu.ruan@bakermckenziefenxun.com

Dom Edmondson
Special Counsel, Hong Kong
IPTech
+852 2846 1652
dominic.edmondson@bakermckenzie.com

Stephen Crosswell
Partner, Hong Kong
Antitrust & Competition
+852 2846 2599
stephen.crosswell@bakermckenzie.com

Laura Liu
FenXun Partner, Beijing
Antitrust & Competition
+86 10 6535 3865
laura.liu@bakermckenziefenxun.com

Tess Lumsdaine
Partner, Hong Kong
Employment
+852 2846 1608
tess.lumsdaine@bakermckenzie.com

Jonathan Isaacs
Partner, Hong Kong
Employment
+852 2846 1968
jonathan.isaacs@bakermckenzie.com

Andrea Kan
Associate, Hong Kong
Investigations, Compliance & Ethics
+852 2846 1742
andrea.kan@bakermckenzie.com

Yuki Yung
Associate, Hong Kong
Investigations, Compliance & Ethics
+852 2846 2512
yuki.yung@bakermckenzie.com