

The ISO 37008 Internal investigation standard framework and what this means for financial services institutions

Received (in revised form): 29th July, 2024

Steve Young

Chief Executive Officer, ACi, UK

Simon Scales

Chief Education & Development Officer, ACi, UK

Steve Young served 20 years in UK law enforcement investigating economic crime specialising in the proactive investigation of banking fraud, bribery and corruption, whistleblowing and money laundering. This was followed by six years at Citigroup Inc. as EMEA Regional Director of Investigations, and eight years as Barclays Bank Plc, Global Head of Investigations for Investment Banking and Wealth Management. Steve is currently Head of Fraud and Investigations in Group Compliance at Lombard Odier, based in Geneva. To date, he has 44 years of international economic crime experience in both a law enforcement and corporate environment.

Simon Scales's extensive international experience in corporate investigations includes significant employee misconduct, fraud, bribery, corruption, antitrust and competition, anti-money laundering, sanctions, market abuse and commensurate preventative/remedial measures. His 40 years of expertise in major investigation management, covert and overt intelligence gathering, relationship and stakeholder management, ethics/compliance/integrity-related investigations and reviews demonstrate his proven ability to facilitate consensus through negotiation and collaborate with senior management and stakeholders.

ABSTRACT

ISO 37008 provides companies with a way to standardise their reporting and investigations protocols while providing a framework to tailor these processes to manage key requirements in new and

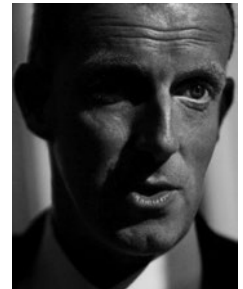
existing compliance and ESG regulations. The Association of Corporate Investigators (ACi) played an integral part in developing this ISO 37008 'Internal Investigations of Organizations — Guidance', which looks at the full cycle of an internal investigation for organisations. It covers the establishment of investigative policies and procedures, implementation of the investigation process, the reporting of the investigation result and the performance of remedial measures. Readers will see that financial services institutions of all types and sizes may have occasions where they want to set up an internal investigation. This may be necessitated by matters coming to their attention that require immediate response and include internal misconduct, significant financial irregularity and risk, together with compliance breaches. An internal investigation which is properly carried out may help organisations negate or mitigate the effects, and with the foresight gained through an investigation, an organisation can then develop timely remedial measures to resolve these breaches. This ISO standard lays out the essential aspects of an internal investigation with a view to practical application and overlays the ACi Investigation Principles. Drafted generically, it can be tailored to meet different organisational needs, and a detailed case study helps to guide readers through the benefits of setting up a well-rounded investigative process ready to be deployed when breaches happen.

Keywords: ISO 37008, investigations, governance, compliance, risk

DOI: 10.69554/ISAU3985



Steve Young



Simon Scales

ACi,
Kemp House,
152-160 City Road,
London, EC1V 2NX,
UK

Tel: +44 7881 517156;
E-mail: steve.young@my-aci.com

Tel: +44 7990 550030;
E-mail: simon.scales@my-aci.com

Journal of Financial Compliance
Vol. 8, No. 2 2024, pp. 181–192
© Henry Stewart Publications
2398-8053 (2024)

INTRODUCTION

The Association of Corporate Investigators (ACi) contributed, as experts, to the drafting of the International Standards Organisation's (ISO) 'Internal Investigations of Organizations — Guidance' (ISO 37008). The guidance was published in July 2023. The guidance forms part of the ISO 37000 range of ISO guidance which include:

- ISO 37000 'Governance of Organizations';
- ISO 37001 'Anti-Bribery Management Systems';
- ISO 37002 'Whistleblowing Management Systems';
- ISO 37003 'Fraud Control Management Systems';
- ISO 37004 'Governance Maturity Model';
- ISO 37005 'Developing Governance Indicators';
- ISO 37006 'Effective Organisational Governance';
- ISO 37007 — Pending;
- ISO 37008 'Internal Investigations of Organizations';
- ISO 37009 'Conflict of Interest in Organizations'.

The 37000 series of ISO publications falls within the remit of ISO Technical Committee (TC) 309.¹ 'TC 309 Governance of Organizations was established in September 2016 to address "standardization in the field of governance relating to aspects of direction, control, and accountability of organizations"'.

It must be noted that the documents in the ISO 37000 series are guidance documents and not standards *per se*. It would be fair to say that within financial services institutions there are 'believers' and 'non-believers' in ISO standards and guidance documents, primarily due to a number of deeply entrenched methodologies led by those without a clear mindset for change. For example, many financial services institutions follow the guidance provided in ISO 37301 'Compliance Management Systems' and feel that this

is sufficient to provide guidance for establishing, developing, implementing, evaluating, maintaining and improving an effective and responsive compliance management system within organisations. Compliance (in the context of ISO 37301) is not an 'investigation', however, with good governance and compliance seeking to give comfort to what 'should be', as opposed to having to investigate an issue or concern as a result of poor governance or control weaknesses. Following the guidance in the 37000 series of guidance documents supports the overall objective of maintaining a robust overall compliance programme, and ISO 37008 enhances the investigative element.

As financial services institutions fall with the regulated sector, they should find that following ISO 37000 series guidance adds to the armoury of (and approach to) the three lines of defence² model as a further tool to strengthen the organisations overall risk, control and governance environments.

WHAT IS AN INTERNAL INVESTIGATION?

Investigations are a reality for financial services institutions. Any organisation — small, medium or large — will find itself having to conduct internal investigations into a wide range of issues or, indeed, may need the services of external providers to do this for it. The ISO guidance states an investigation is an integral part of organisational management — a professional fact-finding process, initiated by (or for) an organisation, to establish facts in relation to alleged or suspected wrongdoing, misconduct or non-compliance (such as bribery and corruption, fraud, bullying and harassment, violence, discrimination or indeed other breaches of an organisational code of conduct). In the financial services sector, the word 'investigation' can be found in many contexts. For example, in banks, payment operations can investigate error payments or

transaction monitoring teams can investigate transaction monitoring alerts. Nevertheless, the word investigation is more commonly associated with allegations of wrongdoing, misconduct or non-compliance, all of which sit clearly within a background of governance or business integrity.

The functions and tasks financial services institutions apply to the word ‘investigation’ is part of the reason clarity is needed in the organisation’s governance documents.

WHAT DOES GOOD INVESTIGATIVE GOVERNANCE LOOK LIKE?

ISO 37008 speaks to the need for organisations to have a clearly defined and written investigations policy or procedure. In reality, financial services institutions as a regulated sector will need both.

If the ISO standard is considered in the context of what financial services institutions should think about when considering good investigative governance, the following key questions arise:

- If the financial services institution has an investigative function, where does the function sit in the organisational structure?
- If the financial services institution is a small or medium-sized business and contracts out investigations to external providers, how is the management of investigations covered in the governance model?
- As almost all financial services institutions operate the three lines of defence model (a model for managing risk and controls in organisations), which line of defence in the organisation is best suited to house the investigative function?
- Who is the accountable executive at executive committee level responsible for the investigation function?
- How are significant investigations reported to the board?
- As the financial services institution is in the regulated sector, are there regulatory rules or guidance that must be followed in the jurisdictions in which it operates?
- Is the reporting line for the head of the investigations function clear, and does it involve matrix reporting lines?
- Is the mandate for the investigative function clear and documented in policy?
- Which oversight committee(s) have responsibility for investigations in their terms of reference?
- What investigations management information (MI) do they require, and do they have rights of challenge?
- Is the remit of the investigations function clearly defined in terms of matters it is charged to investigate under its responsibility?
- If a case triage process exists to refer cases to other functions or externally, is this clearly documented in a policy, procedure or process document?
- Do functions mandated to undertake different types of investigations have suitably qualified and skilled staff to undertake investigations?

These are all fundamental, and the list is not exhaustive. It is, however, thought-provoking when addressing investigation governance needs.

Financial services institutions commonly have their investigative function seated firmly within an audit or legal reporting line. However, this does not necessarily suggest that the reporting line means that there is no presence at board level, and this is often managed through an accountable executive who is responsible for the function, albeit the head of investigations has a line of sight to the board and indeed any supervisory board or non-executive directors. This provides the necessary comfort and assurance, and some organisations have created a business integrity function which embraces both the investigative and whistleblowing management functions.

The ACi advise the following investigations governance documents for financial services institutions:

- *charter* or similar document, with the investigations mandate and details of who is responsible for investigations.
- *investigations policy* which covers the remit, case triage and allocation process, together with who holds the responsibility for investigating cases of varying types;
- *investigations procedures manual* which outlines the procedures investigators must follow when conducting investigations;
- *oversight committee(s)* terms of reference and reporting requirements (management information) for investigations;
- *investigation response plan* for significant cases meeting materiality thresholds determined by the financial services institutions in accordance with its risk appetite;
- *investigation function process* documents for internal processes and templates for investigation plans, for recording the scope, investigative actions, timelines and final reports.

It is important financial services institutions draft and apply investigation governance documents that are aligned to the existing organisational governance models. The documents are not intended to replace or sit outside an existing framework but should complement such a framework by being relevant to the investigation space. Regulators look for a clear delineation of roles and responsibilities for financial service institutions operating a three lines of defence model.

ADOPTING AND APPLYING 'PRINCIPLES'

Many financial services institutions have openly stated the values and behaviours which they apply when conducting business and codes of conduct applicable to their employees (including third parties and contractors). Those responsible for conducting

investigations — especially into members of staff — are expected to apply the highest levels of ethics and integrity.

ISO 37008, Section 4 sets out five key principles which should be applied to all investigations regardless of type:

- independent;
- confidential;
- competent and professional;
- objective and impartial; and
- legal and lawful.

In accessing what the guidance means for financial services institutions, the adoption of these investigation principles would have no downside.

THE INVESTIGATION PROCESS

ISO 37008 sets out a process which can be applied to investigations. It is neatly summarised in Figure 1.

Section 8 of the ISO 37008 guidance presents a helpful investigation process many financial services institutions with dedicated investigation teams will be familiar with. Assessing what it means is a more focused and robust procedure and process for the conduct of investigations.

WHAT SUPPORT IS OFFERED FOR INTERNAL INVESTIGATIONS?

ISO 37008 addresses the support organisations are expected to provide and include but are not limited to personnel, financial, technical and organisational infrastructure. These resources can be provided internally or externally, with many institutions focused on cost. The use of technology during investigations, especially in the areas of data mining, searching and e-discovery, may well result in significant cost savings in the longer term and, together with the increasing use of artificial intelligence (AI) in the investigations space, adds value in

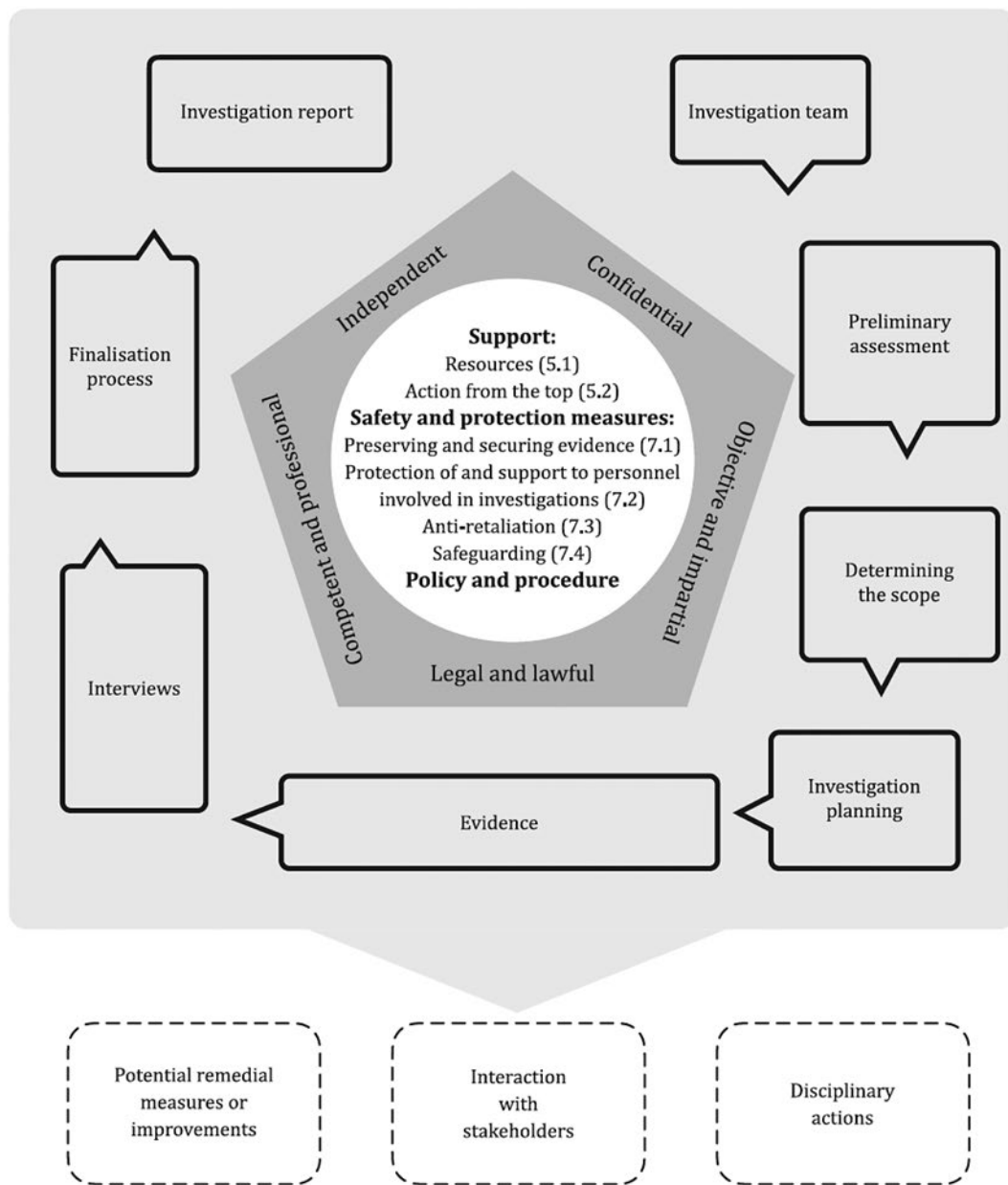


Figure 1 Overview of the investigative process

terms of search speeds, efficiency and accuracy. Depending on the size of the financial institution and case volumes, investing in investigations technology remains a judgment call in terms of the return on that investment in a marketplace that is increasingly growing in terms of new products.

Financial services institutions also need to consider the benefits of contracting out investigations to external providers, such as law firms and consultancies. Contracting out the forensic elements of any case to specialist forensic companies with specialist tools may well prove highly productive in the long

run, as such technology may not be available in house. Indeed, in certain circumstances financial services institutions may decide to contract out the entire investigation to an external law firm. This is a consideration when legal privilege needs to be applied over investigation-related legal advice and when litigation is contemplated. A further consideration is a case for which self-reporting to the authorities is advised and working with regulators and investigative authorities in (for example in bribery and corruption cases).

WHERE DOES 'PROTECTION, SAFEGUARDING AND ANTI-RETALIATION' FIT IN FOR THOSE IMPACTED BY INVESTIGATIONS?

ISO 37008 addresses the protection, safeguarding and well-being of all persons involved in the investigation process, in particular, whistleblowers, who raise concerns and in many jurisdictions are afforded protection under the law. Apart from any legal or regulatory obligations to protect whistleblowers, financial services institutions should ensure they promote a 'speak-up' culture and a tone from the top which encourages staff to raise concerns directly with their line manager or via the whistleblowing channels provided by the organisation (internally and/or externally). This should include (unless prohibited by law) a channel for anonymous whistleblowing.

Financial services institutions should ensure that those charged with undertaking investigations are professionally managed as investigations can be a demanding and challenging area in which to work. This is clearly necessary where cases involve serious wrongdoing, which can include criminal behaviour, and often where members of staff, particularly those in senior roles, are involved. Investigators should be free from bias or influence, especially in cases that have a significant impact on the organisation's revenue and profitability. They should investigate without fear or favour and be

confident in the organisation's support from the C-suite in the event of undue pressure from business management.

Those who manage investigations should be appropriately trained and versed in identifying signs of stress in those charged with conducting investigations and in managing staff in high pressure and time-sensitive roles. The mental health and well-being of all colleagues is a priority and particularly so when a high-profile investigation is taking place within a financial services institution.

WHAT DOES ISO37008 CONSIDER REGARDING 'CONTROL IMPROVEMENTS' (OR THEMATIC/ LESSONS LEARNED) AND STAKEHOLDER ENGAGEMENT?

ISO 37008 recognises the importance of lessons learned from investigations and the importance of improving the control environment. Financial services institutions can benefit greatly from control weaknesses identified during the course of investigations and associated remedial recommendations and actions.

It is important that any control gaps identified during the course of an investigation are closed immediately and legal, risk and compliance experts do not wait for the conclusion of the investigation to take action. This also applies when remediation is identified and required. In the area of financial crime compliance, this has potential regulatory impacts; hence the key message is 'don't wait, and act promptly'.

The guidance recognises the need for effective stakeholder engagement within organisations. Financial services institutions have many moving parts, with many teams often working in silos. An effective investigation requires honest communication and engaging with many stakeholders at all levels with the financial institution. For significant investigations, the investigation response plan should provide a template for success.

WHERE DOES THE INVESTIGATIVE FUNCTION BEST SIT IN AN ORGANISATION?

As the result of the ACi participation in the drafting of ISO 37008, and following its publication, some financial services institutions sought a view from the ACi on a range of investigative issues. Indeed, the two most frequently asked questions were whether the investigative function should be centralised (or not) and where is an internal investigative function best ‘housed’ (in terms of reporting line).

The centralisation of an internal investigative often considers the question of what type of investigation is being conducted. For example, financial crime requires a different set of investigative disciplines from those required for senior leadership misconduct, although both are ‘investigations’ *per se*. The range of skills may lead more naturally towards compliance in the case of financial crime and potentially human resources (HR) for misconduct matters. Indeed, matters relating to sanctions, anti-money laundering (AML) or bribery and corruption can be within the remit of specialists within financial crime compliance.

External fraud investigations are often managed internally through operational risk teams, with internal fraud and serious employee wrongdoing frequently housed within specialised and dedicated investigation teams or within internal audit. Breaches of organisational codes of conduct and expected employee values and behaviours generally sit within HR.

Simply put, investigations are often not a ‘one-size-fits-all’.

The ACi promotes the benefits of a centralised team that is able to provide investigative support to specialists for all investigations. The primary benefit of this is to ensure good investigative efficacy and solid best practice and, fundamentally, to develop knowledge and thought leadership from thematic lessons learned and the drive for consistency.

The exact remit of the cases a centralised team should investigate is a matter for each organisation. However the investigations policy should clearly state ‘who does what’. The ACi’s view is that centralisation allows for better concentration of investigative expertise and management, cross-leveraging of investigative resources and standard investigation procedures with dedicated training and a robust and detailed quality assurance programme.

Turning to the question of ‘where’ a function should sit — or reporting lines — in an organisation, the ACi see compliance as the right functional area for investigations. Many organisations refer to this as ethics and compliance or business integrity, but essentially it has a direct line of sight to the very top of an organisation. Fundamentally, the working relationship with legal and risk should be extremely strong. Compliance may well be a second line of defence; however, compliance officers must also consider the risk of individual criminal liability. It is indeed why regulators favour ‘compliance’ as their accountability goes far beyond ‘in-house’ or regulatory sanctions and may well enter the criminal sphere.

ISO 37008: A DETAILED CASE STUDY

Background and context

An eloquent example of success following the implementation of ISO 37008 is to look at a recent review of ISO 37008 within a large and highly successful multinational financial services organisation, beset by a number of investigative challenges following a number of concerns and allegations which were raised against the organisation and its senior leadership team.

Over a five-year period, the organisation faced numerous procedural and internal policy challenges surrounding its internal investigations process. This followed a regulatory investigation which, while finding the concerns unsubstantiated, commented

on the lack of updated relevant processes and policies, and that necessitated a thorough review and overhaul.

Predominantly operating in the EU and before adopting the ISO standard, the organisation confirmed that it had experienced a number of inconsistencies within its processes, leading to a perceived lack of transparency and prolonged case life cycles; mainly as a result of failing to have a clearly defined decision and action logging process. The organisational leadership team welcomed a root and branch review in order to support deeper learning and any corrective actions necessary.

After implementing ISO 37008, a notable transformation occurred within the investigation process. Standardised, and fundamentally 'business agreed' procedures incorporated the clear guiding investigative principles, which afforded greater consistency and efficiency within internal investigations. All of these were reinforced through ACi learning and thought leadership. Training became a clear bedrock for change and the introduction of new and updated methodologies improved the quality of triage, assessment and fieldwork enquiries. Additionally, the implementation of technological enhancements streamlined eDiscovery and data collection/analysis processes, which had been clearly lacking focus within internal investigations, where the reliance had been on third parties providing such services who lacked the detailed and deeper understanding of concerns within supporting business functions.

Crucial to the success of onboarding the ISO 37088 standard was the training and development of competent investigators which not only encompassed the core investigative team, but also drew in a mix of colleagues from HR, legal, compliance and business integrity. All may have played a part in previous investigations, whether directly or by being co-opted, and were included as a result of their individual roles, skill sets and expertise. The organisation invested in numerous investigative related

training programmes, from the effective triage and assessment of allegations, the planning and development, how to conduct trauma-informed interviews with reporters, witnesses and subjects, key report writing skills and the management of key internal and external stakeholders. Governing principles were fundamental to the company's success, with each practically applied in all cases and matters under investigation.

Overall, key investigative skills were strengthened and enhanced with a culture of continuous professional learning and development embedded and knowledge and thought leadership crucial to the success of thematic learning shared. The standard reviewed all elements of procedural change, and the results were impressive. Improved investigative efficiencies were found in many areas, including the development and use of e-discovery technology (in house) and specialised investigative tools for use during interviews (contemporaneous notes taken from digitally recorded interviews). Case management systems and reporting tools were improved, together with disclosure protocols for used and unused materials driven by further streamlined collection, analysis and documentation of evidence/data.

Deep thematic learning followed, with the ability to track cases, concerns and allegations more accurately, share information more securely and generate more concise investigation reports, which were still highly detailed in many cases, all leading to more informed and focused decision making.

Nevertheless, there were challenges faced. The most frequently observed was a resistance to change from experienced investigators, who '*had always done things their way*' and were reluctant to consider new ways of working with a view to increasing efficiency. Overcoming this took time and effort, and there was a real need to be open and honest with each other. To complement the process, awareness programmes, enhanced effective communication and the

longer-term benefits of change were slowly and deliberately introduced.

Technology also presented its own problems to the organisation. Adapting to (and accepting) innovative technology met with resistance in the learning curve. This necessitated detailed and informative training sessions, a 24-7-365 approach to technical support for investigators and, above all, a continuous drive by senior leaders to push for change.

Having been through the process of implementing the standard, the procedural and policy enhancements, training, technical integration and overcoming various challenges have ensured that the organisation has strengthened its ability to manage investigative risk, has become even more regulatory compliant and, above all, is continuously improving within the entire case life cycle. The ISO 37008 framework has enhanced and elevated trust in the internal investigative process, supported the organisational governance and compliance aims and overall has meant that concerns and allegations are dealt with quickly, robustly and effectively, which has instilled a far deeper culture of trust and openness in the organisation.

Why was ISO 37008 chosen as a framework?

Simply put, following the news in July 2023 that ISO 37008 had followed a two-year process involving experts from different countries, the standard for the internal investigations of organisations was seen to be the most effective driver for change.

As a global standard, ISO 37008 reflects international best practices for internal investigations conducted in corporates and multinationals across the world, and this includes financial services institutions. By design, it appeals. The standard can be used and adopted by any organisation, irrespective of size, and in any country as the standard is

malleable to size, industry/segment, structure, governing body, regulatory focus and type of concern or allegation. Knowing that internal investigations should be conducted independently and in an objective and impartial manner, the organisation was aware that, at its core, it already had competent and professional investigators who managed and applied an attention to detail that would be seen as commensurate with applicable law(s) while maintaining confidentiality. But this was not enough.

The standard was noted for being able to facilitate interaction with internal and external stakeholders, with clearly defined procedural recommendations, including the main aspects of cooperation with regulators and other (enforcement) authorities. Incorporating matters that might require regulatory disclosure into a more robust framework was seen as crucial to new ways of working and required the support and leadership of the organisation to drive the standard forwards, together with the application of revised policies, processes and procedures.

A closer examination

The organisation closely compared existing procedures with the benefits achievable with ISO 37008 before embarking on change. This is noteworthy in terms of understanding what this means for the wider financial services community irrespective of organisational size and whether scalable change is possible. Identifying the occasions when internal investigations are required and change would benefit the process necessitated a change of approach for matters arising through internal ethics, compliance, governance or whistleblowing activity and requiring immediate response. The initial signs were promising, and the overall result was outstanding.

Regulatory scrutiny on certain matters — both financial crime and associated senior misconduct — focused the attention and

conversations, with substantial improvement seen in the overall reduction of risk, whether financial or reputational. Thematic learning and thought leadership lessons shared learning with those making — and taking — corrective action, in order to ensure the lessons learned had practically applied mitigations and solutions to support the organisation.

The ISO standard provides the framework and the essential aspects of any investigation. If followed, it should satisfy all organisational requirements. While drafted generically, it was tailored to the organisation and its specific needs with a simple, ready-made and deployable process without significant cost. This approach is often lacking in many organisations, and the ISO standard applied in this instance has now highlighted the simplicity of application for many others as a highly effective model.

As the standard provides guidance on the life cycle of an internal investigation (the design and implementation of relevant investigative policies and procedures, investigation frameworks, recommended reporting practices following completion and the oversight and ownership of remedial measures) the organisation embarked on a 'total framework review' encompassing all elements of the standard. Specific focus was given to the principles adhering to:

- independence;
- confidentiality;
- competence;
- professionalism;
- objectivity;
- impartiality; and
- legality.

These seem to be the most crucial for the organisation.

While the application of these principles was, in the main, relatively organised, it was seen as disparate with competing

influences at many stages of the internal investigation life cycle. While most stood the test of acceptability, it was definitely at 'bronze standard' level as opposed to 'gold' or 'platinum'. Widespread improvement was achievable in all life-cycle pillars, including triage, assessment, fieldwork, interviewing and reporting. Key to the success of implementation was to follow the guidance and standards taken from the 'Uniform Principles of Investigations and Good Practice Guidance' issued by the ACi.³ The standard's emphasis on senior management support during internal investigations provided a splendid bedrock on which the investigative function could rely, with a keen desire to learn far more from examples of potential misconduct, regulatory compliance and other concerns and allegations. This was crucial to the embedding of not only new ways of working but also a cultural change within the organisation.

Among the areas identified requiring change were:

Pre-investigation stage: A lack of understanding at the preparatory stage led to confusion as to what exactly would be investigated, and what policy, process or law this was in breach of. The triaging and assessment of concerns required revision. The concerns were previously made to 'fit' case management system identification (eg 'pigeon-holing' matters) as opposed to satisfying clearly identifiable concern data, and investigation teams were not mobilised to consider skills and expertise together with learning. An attitude of 'I've done this before, so I'm best suited to do it again' led to a silo mentality. Case and thematic learnings were not shared, and therefore, a way to mobilise the most effective investigation team was necessary.

Fieldwork (and the conduct of the investigation): Methodology flaws were identified in the stages of preservation of evidence, protection afforded to those reporting (including witnesses) and the prevention of interference

with the investigation process. Also required was an appropriate document management approach, together with the maintenance of a 'decision and action log' which clearly stated actions taken and any deviation from process. While the interview process was relatively sound, the introduction of a methodology to address audio and video recording of interviews was required. Such recordings often provide the most crucial evidential value and are an essential pillar of any successful investigation. Document management and e-discovery processes were acceptable, largely centred around the identification and preservation of essential documents and evidence, although these were mostly handled by third party providers. The organisation was keen to bring this activity in-house. All contributed to a well-considered and documented final investigation report, with report writing skills requiring training and education for all authors.

Post-investigation stage: It was the change to reporting at the final investigative stages that proved to be the most crucial element for post-investigative efforts. Improved reporting led to clear, accurate and easily applicable remedial measures to be recommended. These ultimately led to an improved overhaul and adjustment to the organisation's existing compliance structure. Crucial decisions by the organisation's senior management were better understood, including whether to self-report breaches to the relevant authorities, something which had previously faltered. The interaction with external stakeholders and remedial measures required to address the situation were seen as fundamental to organisational investigative improvement and strengthened resilience against potential financial and reputational risks.

THE OVERALL BENEFITS

Adopting ISO 37008 realises substantial benefits to any internal investigative

function, whether independently operated or forming part of an ethics, compliance, governance or business integrity function. The standard provides a highly robust and solid procedural framework, ensuring best practice, consistency and quality assurance throughout all investigative phases.

In this instance, by following the ACi guiding principles and those adopted within ISO 37008 the organisation significantly enhanced all areas of investigative effectiveness from the receipt of concerns and allegations to triaging, assessment and initial identification to investigation, resolution and follow-up. Furthermore, the standard acts as a primary guardian and internal verifier of any ethics and integrity programme, establishing clear guidelines for investigative conduct, reinforcing internal and external trust with key stakeholders and strengthening the organisation's position against potential regulatory, legal and reputational challenge.

THE ACi GAP ANALYSIS

As the implementation process of the standard is a methodical and structured pathway towards investigative excellence, it begins with a thorough assessment and gap analysis of existing related processes, identifies areas for improvement and aligns them with the ISO standard requirements. A clear action plan is developed to ensure that roles, responsibilities and investigative deadlines are agreed, with the emphasis on developed learning and thought leadership through relevant training to ensure those investigating understand and adhere to the standard.

Something that is important here is the correct documenting of policy and procedures, with a robust case/investigative management system being essential to ensure operational investigative integrity. It is driven by what currently exists; it is not a rewrite of existing policy and process but a simple audit of

processes and gaps which leads to the management of effective investigative efficacy and the benefits of external certification, ensuring that the organisation complies with the rigorous standards of ISO 37008. The standard not only establishes the correct guidelines for effective management of internal investigations but also plays a crucial role in managing risk, and the requirements of regulatory compliance.

Organisations that consider a gap analysis and adopt ISO 37008 are able to demonstrate their enhanced ability to identify, assess and mitigate internal investigative risks, thereby creating an environment where an agile and efficient response to potential threats is always in place, from the receipt of concerns through the case life cycle to reporting.

Regulatory compliance is satisfied by ensuring that ethical, compliant and legal

guidelines for internal investigations are maintained, particularly where the matter is the subject of legal privilege. This helps to avoid potential sanctions and penalties and also thoroughly reinforces the integrity of investigative and business practice.

REFERENCES

- (1) ISO/TC 309 (n.d.) 'Home Page', available at <https://committee.iso.org/home/tc309>.
- (2) Institute of Internal Auditors (2020) 'The IIA's Three Lines Model: An Update of the Three Lines of Defense', available at <https://www.theiia.org/globalassets/site/about-us/advocacy/three-lines-model-updated.pdf> (accessed 13th September, 2024).
- (3) Association of Corporate Investigators (2023) 'The ACi Corporate Investigators Handbook', available at <https://globalinvestigationsreview.com/guide/the-aci-corporate-investigators-handbook-in-association-gir/first-edition> (accessed 13th September, 2024).