THE GUIDE TO COMPLIANCE

SECOND EDITION

Editors
Johanna Walsh, Alejandra Montenegro Almonte and Alison Pople KC

Guide to Compliance

Second Edition

Editors

Johanna Walsh

Alejandra Montenegro Almonte

Alison Pople KC

Published in the United Kingdom by Law Business Research Ltd
Holborn Gate, 330 High Holborn, London, WC1V 7QT, UK

www.globalinvestigationsreview.com

Enquiries concerning reproduction should be sent to: insight@globalinvestigationsreview.com.
Enquiries concerning editorial content should be directed to the Publisher –
david.samuels@lbresearch.com

ISBN 978-1-80449-257-4

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

Acknowledgements

The publisher acknowledges and thanks the following for their learned assistance throughout the preparation of this book:

Ankura Consulting Group, LLC

Baker McKenzie

Beccar Varela

Cloth Fair Chambers

Davis Polk & Wardwell LLP

Debevoise & Plimpton LLP

Demarest Advogados

Freshfields Bruckhaus Deringer

Galicia Abogados, SC

Herbert Smith Freehills

Jenner & Block LLP

Miller & Chevalier Chartered

Mishcon de Reya LLP

QEB Hollis Whiteman Chambers

Ropes & Gray International LLP/R&G Insights Lab

Wells Fargo

Publisher's Note

The Guide to Compliance is published by Global Investigations Review (GIR) – the online home for everyone who specialises in investigating and resolving suspected corporate wrongdoing. We tell our readers everything they need to know about all that matters in their chosen professional niche.

Thanks to GIR's position at the heart of the investigations community, we often become aware of gaps in the literature first. *The Guide to Compliance* is a good example. For, although there has been significant growth in guidance on compliance worldwide – and a change in attitudes towards compliance on the part of enforcers (namely that 'good' compliance programmes can still fail) – to date, there has been no systematic guide to how exactly compliance fits into the enforcement equation, or how an organisation can demonstrate that it took compliance seriously. This book aims to solve that.

It combines a systematic *tour d'horizon* of the rules in place around the world with specific practical advice and a scan of the horizon in parts two and three. As such, it should swiftly earn a position in the front row of our readers' libraries.

The guide is part of GIR's steadily growing technical library. This began seven years ago with the first appearance of the revered GIR *Practitioner's Guide to Global Investigations*. *The Practitioner's Guide* tracks the life cycle of any internal investigation, from discovery of a potential problem to its resolution, telling the reader what to do or think about at every stage. Since then, we have published a series of volumes that go into more detail than is possible in *The Practitioner's Guide* about some of the specifics, including guides to sanctions and to monitorships. I urge you to seek out all of them.

If you are a GIR subscriber, you will have received a copy already, gratis, as part of your subscription. If you are not, you can read an e-version at www.globalinvestigationsreview.com.

Last, I would like to thank the editors of *The Guide to Compliance* for bringing us this idea and for shaping our vision, and the authors and my colleagues for the elan with which it has been brought to life.

We hope you find the book enjoyable and useful. And we welcome all suggestions on how to make it better. Please write to us at insight@globalinvestigationsreview.com.

David Samuels
Publisher-at-large, GIR
September 2023

Part II

Compliance Issues in Practice

CHAPTER 11

The Role of Audit and Monitoring in Compliance

Jean-Michel Ferat and Shelly Mady[1]

Internal audit and monitoring functions are important to an organisation's ability to design and implement an effective compliance programme. Although each function has a distinct mandate, both contribute to the organisation's ability to understand its compliance risks, tailor its compliance programme to those risks, and continually reassess and improve its internal controls to respond to an ever-changing compliance landscape. Ultimately, the presence, empowerment and performance of these functions contribute to sentencing and post-event outcomes.

Regulator expectations

Regarding sanctions and other enforcement action, global standard setters (such as the Organisation for Economic Co-operation and Development) recommend that countries incentivise 'good corporate behaviour' by considering mitigating factors such as fulsome, timely and voluntary disclosures of misconduct, acceptance of responsibility and the implementation of an effective compliance programme.[2] In the United States, sentencing guidelines for organisations require any fines imposed to be based on both the seriousness of the offence and the culpability of the organisation. A court's assessment of culpability is determined by six factors, two of which mitigate the ultimate punishment of an organisation: the existence of an effective compliance and ethics programme, which includes monitoring and

1 Jean-Michel Ferat and Shelly Mady are senior managing directors at Ankura Consulting Group, LLC.

2 Organisation for Economic Co-operation and Development, 'Recommendation of the Council for Further Combating Bribery of Foreign Public Officials in International Business Transactions', Sanctions and Confiscation: Article XV.

auditing to detect criminal conduct, and self-reporting, cooperation or acceptance of responsibility.[3] In the United Kingdom, prosecutors assign similar importance to the design of an organisation's compliance programme and its willingness to self-report.[4] Often, an organisation's ability to self-report is dependent on effective operation of its gatekeeping and defence functions – most notably internal audit and monitoring.

Risk-based auditing and monitoring as components of an effective compliance programme

US regulators tend to evaluate programmes using three enquiries: 'Is the company's compliance programme well designed? Is it being applied in good faith? Does it work?'[5] The presence of effectively operating internal audit and monitoring functions contribute to the design and implementation of an effective compliance programme and allow an organisation to assess its effectiveness.

Effective compliance programmes are grounded in a robust risk assessment, one that is best informed by well-functioning internal audit and monitoring processes, because risk assessments help an organisation tailor its compliance programme to its size and scope. Although strategies and procedures can be similar, there is no such thing as a one-size-fits-all approach to compliance – a fact recognised by most practitioners, government agencies and international bodies, such as the United Nations;[6] however, as an organisation's compliance risks increase, so should the resources devoted to auditing and monitoring.[7]

An organisation's assessment of risk also allows it to focus resources on higher risk markets or transactions. Regulators in the United States and the United Kingdom recognise that companies have limited resources and that a decision to focus on a higher-risk area based on the company's risk assessment may result in the lack of prevention of an infraction in a low-risk area. Despite this fact pattern, companies subject to enforcement actions may still receive credit for having an

3 US Sentencing Commission, Guidelines Manual , Chapter 8 – Sentencing of Organizations.

4 Crown Prosecution Service (CPS), 'Bribery Act 2010: Joint Prosecution Guidance of The Director of the Serious Fraud Office and The Director of Public Prosecutions' (the Bribery Act 2010 Guidance).

5 US Department of Justice (DOJ) and US Securities and Exchange Commission, 'A Resource Guide to the U.S. Foreign Corrupt Practices Act', 2nd edn., July 2020 (the Resource Guide).

6 United Nations Convention Against Corruption, Article 12(f).

7 Resource Guide; Bribery Act 2010 Guidance.

effective compliance programme; however, organisations that fail to understand their risks and focus resources accordingly may receive less credit for the quality and effectiveness of their programmes.[8]

Regulators also expect effective compliance programmes to incorporate continuing monitoring of third parties.[9] To do so, an organisation needs to understand the landscape – and, most importantly, where the risks reside – of its third-party relationships. A meaningful risk assessment informs a company's understanding of third-party risk, but auditing and monitoring facilitate the processes that keep that risk assessment current along with periodic due diligence updates, exercise of audit rights, training and tracking of annual certifications.

Most importantly, regulators expect effective compliance programmes to embrace the idea of continuous improvement, and auditing and monitoring processes drive the feedback loop. As a company's business, regulatory requirements, customers and environments change, so must its compliance programme.[10] Organisations must review and test their controls and processes to ensure not only that they are working as intended but that they are aligned with the company's risks.

Auditing versus monitoring

Although both auditing and monitoring drive the risk assessment needed to develop, implement and improve effective compliance programmes, each function is distinct in its structure and aims. Traditional auditing functions are more structured and systematic in their approach and are designed to evaluate effectiveness of controls, determine the root cause of identified failures and drive improvements in a company's control environment. Audit exercises assess controls at a specific point in time and are performed retrospectively by individuals or teams independent of the process being examined.

Where within the organisation an auditing function is housed may depend on the organisation's size, scale and risk profile. Some organisations choose to audit compliance processes with a dedicated compliance audit function. Others perform those same activities under the umbrella of a more traditional internal audit group. Regardless, audit activities are more formal in nature.

8 id.

9 id.

10 Bribery Act 2010 Guidance.

In contrast to audit, monitoring exercises are meant to assess the design and effectiveness of key compliance and internal controls by taking a more real-time, continuing approach. Although audit exercises typically rely on established sampling methodologies and transaction testing to drive their assessment, monitoring can be enabled by continuous data analysis.

Whether conducted by a compliance team or the business itself, monitoring offers a less rigid approach to driving improvements to an organisation's compliance programme through identification of trends and findings at a more holistic, organisational level. Key to effective monitoring is an organisation's ability to leverage existing sources of data and design protocols to respond to and highlight areas of risk. Ultimately, monitoring procedures designed to assess transactions provide insight into the effectiveness of compliance-related internal controls.

Auditing and monitoring working in tandem

Differences aside, auditing and monitoring processes can work hand in hand to help an organisation understand its risk landscape and allocate resources accordingly. Trends observed at the organisational, regional or country level can point to an area where a company may want to dig deeper in the form of a process audit. For example:

- trend analyses facilitated by monitoring that identify a spike in the number of third-party sales agents in China may prompt a company to plan an audit of third-party onboarding and due diligence practices in the region;
- an increase in consulting expense in Africa may elicit a review of documentation supporting the performance of services and the underlying contracts; or
- a noticeably higher level of discounts issued for products sold to distributors in one country as compared with another may point to the need for an audit of pricing and discounts.

Examples in practice

The following two examples of enforcement actions illustrate how proper monitoring protocols or audit exercises may have helped to detect and mitigate the issues encountered.

In the first example, a large multinational technology company paid approximately US$40 million to two consultants in Saudi Arabia on the understanding that these consultants had influence over Saudi state-owned telecommunications company officials making decisions on contracts. The company signed consulting agreements knowing that the services would never be performed, and the company completed due diligence on the consultants one year after the agreements had been signed only because it was required to complete payment. Given the high

risk associated with government contracting, a monitoring protocol designed to flag statistically significant time lags between contract effective dates and due diligence completion or first instance of payment might have identified the improper payments earlier. Transaction testing during an audit of the company's Saudi entity, while less real-time, may have identified that payments had been made without evidence of performance of services.

In the second example, a global aircraft manufacturer engaged and paid a consultant to facilitate and conceal bribe payments made to government officials in Ghana to secure government contracts for the acquisition of aircraft and aircraft parts. To conceal the payments to the consultant, the manufacturer avoided paying the consultant directly and instead made payments to another organisation, based in Spain, which then transferred the funds. In this case, the industry of the manufacturer, the nature of the underlying services and the location all contributed to the transactions' higher risk level. A monitoring protocol designed to identify cross-border payments may have identified the mismatch between the location of the payee organisation and the fact that the payments were for services provided in Ghana. An audit of the transactions themselves might have identified that the first underlying contract had been backdated and falsely stated that the organisation had operations in Spain or that subsequent payments had been made without a renewed contract in place.

Connection between audit, monitoring and risk assessment

As discussed above, organisations must tailor their compliance programmes to address their risks, including those presented by the location of operations, industry sector, competitiveness of the market, regulatory landscape, client profile, number and nature of third-party business partners, and touchpoints with foreign governments and officials. But as the business changes, so must a company's assessment of its risks and, as a result, its compliance programme: neither can be static, and both must evolve based on continuously updated operational data from across the organisation. A company's ability to review its compliance programme and ensure it is not 'stale' can influence prosecutorial decision-making.[11]

Audit and monitoring activities are key to both informing a company's risk assessment and executing control activities to monitor the identified risks appropriately. Risk assessments form the basis of where and how a company allocates resources within audit and monitoring plans at the organisational, regional and

11 DOJ Criminal Division, 'Evaluation of Corporate Compliance Programs', updated March 2023.

local level. Decisions regarding the location and subject matter of audits, the frequency of auditing and monitoring activities, and investments in technology platforms and solutions to enable the monitoring of processes and transactions are all guided by management's understanding and prioritisation of its risks.

Although audit and monitoring plans that focus on high-risk transactions or process areas may not detect or prevent all issues from arising, prosecutors may still credit the quality and effectiveness of a compliance programme if the organisation is able to demonstrate that its decision to focus resources corresponds to its assessed level of risk.[12]

Risk assessments also inform the audience for reporting results of audit and monitoring activities. For example, senior level management may review audit reports from third-party audits performed by sales agents if the organisation has identified related issues in the past, or regional leadership may request to receive monitoring updates on the number of payments processed to consultants if government touchpoints in the region are particularly high.

Organisations also consider industry-wide trends when assessing risk. For example, pandemic-driven supply chain disruptions may require a company to increase the number of third-party suppliers or alter its contracts with existing suppliers. As a response to the increased risk of a larger supplier pool, a company may increase the frequency at which due diligence is refreshed, more closely monitor one-time payments to third parties, or increase the number of third-party compliance audits performed in a given year.

At the same time, results of audit and monitoring exercises should be inputs to the risk assessment itself. Previous audit findings and trends observed across transactions guide management's understanding of where issues have arisen in the past or may arise in the future and influence management's plans to mitigate the related risks. An organisation must have ways of tracking audit and monitoring findings, analysing trends and incorporating what it has learned into its risk assessment to better tailor its compliance programme to mitigate areas of new or increasing risk.

Role of data in monitoring: understanding the technology landscape

Identifying data relevant to compliance monitoring

Critical to a company's ability to perform effective monitoring is the data it collects from all areas of the business. By leveraging data, organisations can monitor large volumes of transactions and process steps efficiently and consistently while reducing the resources needed.

12 id.

Before designing a data-centred approach to continuous monitoring, an organisation must understand its technology landscape and the nature of the data that resides within its systems. Compliance sensitive data can reside in various environments across the organisation, including within enterprise resource planning (ERP) systems, time and expense systems, procurement systems, third-party due diligence platforms, contracts databases and others. As an initial step in the process, the organisation must ask whether it has the data to enable monitoring of its highest risk areas and where that data resides. Cataloguing the existence of compliance sensitive data pools within the organisation is the first step in determining what sources the organisation can monitor in an efficient and effective manner.

The accuracy and integrity of the data itself is critical to the success of any continuous monitoring solution. Equally important to selecting the right data to monitor is the company's ability to ensure data integrity and completeness. For every level of data transformation, enhancement, conversion and transfer, appropriate validations should be built into the process to ensure data integrity from start to finish. The mantra 'garbage in, garbage out' is especially true when it comes to compliance monitoring.

Enterprise resource planning systems

Of all data sources, ERP systems are often the most comprehensive and relevant as they typically house a wealth of data, including sales and expense transactions with third parties. Although some companies maintain one ERP system to serve the entire organisation, making it easier to ring-fence and analyse data, other companies maintain several. Some organisations have vastly disparate ERP landscapes comprising numerous different ERP systems because of geographical diversity, distinct business segments with differing operating needs, or a failure to integrate IT systems following acquisitions.

Because an organisation's ERP environment often dictates its ability to effectively and efficiently monitor transactions in a holistic way, the organisation must have an understanding of:

- the number and structure of existing ERP systems;
- availability of off-the-shelf monitoring tools capable of handling those systems;
- the ability and institutional appetite to build in-house or custom monitoring solutions;
- existing or desired plans to centralise data sources or consolidate ERP systems, including the effort and length of time required to do so; and
- pending merger and acquisition activity and planned integrations of acquired ERP systems and data sources.

The existence of highly decentralised ERP systems may result in the need to consolidate the ERP systems themselves or to devise alternative solutions, such as data lakes, to combine and analyse data in a centralised location. Underlying each of these elements is the location where an ERP system resides within the company's assessed risk landscape; when considering any centralised data monitoring solution or consolidation plan, an organisation should prioritise ERP processing transactions for high-risk countries or business segments.

Disparate ERP environments are inherently higher risk and more complex to monitor and require longer timelines and more expert-level resources and support personnel to implement solutions. An organisation's plan to implement a monitoring tool should be driven by risk, which may necessitate short-term or medium-term interim solutions while a more comprehensive tool is put into place. Although an organisation's decision to embark on costly and lengthy ERP transformations typically rests with the business, finance and technology groups, bringing compliance into the decision-making process is an important consideration, particularly in respect of risk-based prioritisation.

Actioning a data monitoring programme

Understanding data maturity

Continuous monitoring solutions do not come as 'one size fits all'. Central to any successful programme are an organisation's understanding of its data maturity, the ability to right-size the appropriate solution for 'today' and a definition of a road map setting out the solution's 'future state' with identified improvements.

Building any data-forward solution starts with a solid basic structure. Although new technologies rooted in artificial intelligence or machine learning are growing in use and influence, these technologies cannot be implemented successfully without a solid foundation. For companies with little centralisation of data and information, the 'small' goal of bringing together data for a holistic, comprehensive view for the first time can be a monumental improvement and offer new insights into compliance risk and the business itself.

Starting small paves the way for a much more effective and mature programme in the future. Without taking the critical steps to build a foundation, organisations not only waste time and money but sacrifice the future effectiveness of any monitoring solution. That said, monitoring is a journey, not a destination, and any programme should always be built with an eye towards the future and a defined data road map with targeted goals that consider enhanced analytics, additional data feeds and smarter monitoring.

Building smartly (in-house versus third party)

In addition to understanding their information technology (IT) infrastructure, ERP environment and current technology capabilities, organisations also need to decide whether a monitoring solution provided by a third party or built in-house can better address their needs and risks. This decision should be made in consideration of:

- the availability of monitoring solutions provided by third parties in the marketplace and the capabilities of each;
- current IT resources and capacity and the required skills necessary to use or build a solution; and
- budgetary constraints and necessary sponsorship from leadership.

In parallel, organisations also need to consider the benefits and drawbacks of each option as they relate to system flexibility, advanced analytics capabilities, cost and maintenance needs. Determining the most appropriate solution is not a decision that can be made in isolation, and it is important to have the appropriate stakeholders involved from finance, IT, compliance and the business.

Engaging with diverse stakeholders

The process for developing an effective continuous monitoring programme requires cross-functional coordination. It is critical to have open communication with IT, finance, internal audit, legal (investigations) and others to ensure that the compliance monitoring team is up to speed on emerging issues and is building the appropriate monitoring protocols, tests and visualisations. Bringing in a diverse team with a range of subject-matter expertise is key to defining protocols aligned with the organisation's risks that drive meaningful analysis and results. This coordination is important not only during the development stage but also as the solution is under way. Continuous feedback from all stakeholders ensures that emerging risks are monitored in a timely manner and compliance programmes evolve alongside the business.

Designing compliance monitoring protocols

Organisations should align the technical components of continuous monitoring solutions to the risk areas identified in their risk assessments. Regardless of whether a third-party system or an in-house system is implemented, the design of the technical tests, risk-ranking and dashboard visualisations must align with the processes the organisation has prioritised as being at highest risk. More does

not necessarily mean better, and organisations should choose the tests that will ultimately drive the most meaningful results without overburdening compliance teams with an excessive number of transactions requiring review.

Certain monitoring protocols (e.g., those designed in respect of the US Foreign Corrupt Practices Act) might be centred around established finance processes, such as procure to pay, order to cash, financial reporting, or time and expense, and can leverage a risk-based ranking or selection of individual transactions or third parties for review on a comprehensive or sample basis. Dashboard-based reviews are especially useful for identifying anomalies and outliers that may warrant further investigation or consideration by stakeholders.

When building protocols and tests, an organisation should understand (1) which risk or control it is trying to monitor, (2) what data it will be leveraging, (3) which underlying business process generated the data, and (4) what might constitute a potential exception or anomaly. Financial transaction monitoring protocols should be rooted in assessing the adherence to and effectiveness of key controls and should utilise data points gleaned from a variety of sources, including past internal audit findings, SOX[13] exceptions and weaknesses, investigations and related findings. Thought should also be given to how to interpret monitoring protocols both individually and collectively. Although the results of a single test may not elevate a particular transaction above a risk threshold, the combination of various tests together may do so.

Business as usual: building a sustainable monitoring process

Throughout the implementation process, compliance teams should clearly define the purpose of the monitoring, the approach, the use of the tools, team member responsibilities, and how findings are to be investigated and resolved or escalated. Compliance teams should also consider how findings will be aggregated and tracked for documentation purposes as well as for reporting to the wider organisation.

Throughout the life of the monitoring process, the organisation should remain cognisant of the fact that just as the broader compliance programme needs to be flexible and evolve, so should compliance monitoring processes. Organisations that run the same compliance monitoring protocols year in, year out run the risk of losing sight of where and how enterprise risks emerge and retreat.

13 SOX controls are internal controls designed to prevent and detect errors in a company's financial reporting process and are required for compliance with the Sarbanes-Oxley Act ('SOX' for short).

Root cause assessments

As discussed previously, audit and monitoring activities drive a company's risk assessment and enable it to improve its compliance programme by ensuring that the risk assessment remains current. But how a company investigates the root cause of findings identified through auditing and monitoring determines its ability to evaluate and improve its compliance programme and controls in a sustainable, meaningful way. Root cause analyses form the backbone of successful efforts to incorporate feedback into an evolving risk assessment and compliance programme through identification of the processes that may need revision and individuals or organisations that may need to be held accountable for preventing similar issues in the future.

Root cause analysis is a process for both understanding what happened and identifying the solution through examination of what led to the finding in the first place. A well-performed root cause analysis can reduce or eliminate the likelihood that a similar finding happens again by leading to higher impact management recommendations that, if implemented, result in process and programme improvements; however, because problems in complex organisations seldom arise from just a single cause, specificity in root cause analysis is necessary.

Root cause analysis methodology

There are several models an organisation can use to conduct evidence-based root cause analyses, and an organisation can either select the one that best meets its needs[14] or use a combination of methods:

- *The five whys*: Originally developed in the 1930s by the founder of Toyota Motor Corporation, this method is often popular among internal audit groups and involves asking 'why' at least five times to drill down and identify a root cause. This method can identify several root causes and lead to realistic, integrated solutions.
- *Ishikawa diagrams* (fishbone or cause-and-effect diagrams): Like the five whys method, fishbone diagrams became popular after use in the automotive industry. This method begins with a description of the problem, collection and analysis of data, and brainstorming of potential root causes that are first

14 Summarised from Chartered Institute of Internal Auditors, 'Root Cause Analysis', 1 February 2023, www.iia.org.uk/resources/delivering-internal-audit/root-cause-analysis (accessed 11 August 2023).

grouped into major categories (e.g., people, process, environment or other causes) and then distilled into the true root cause. This method is helpful in showcasing that an issue can result from multiple, interrelated root causes.

- *FME*: Originally developed to study malfunctions in military systems, the failure mode effects analysis (FME) is popular in the aerospace and automotive industries. It brings together a cross-functional team that identifies all ways a failure could happen and examines the potential root causes for each one. The team also estimates the probability of the issue occurring, identifies any controls currently in place and estimates how well those controls would detect the issue.
- *Fault tree analysis*: Developed by the military, this method has subsequently been used in the aerospace, chemical and software industries. Fault tree analysis is a top-down approach aiming to simplify the cause of an issue using a graphical model.

Potential challenges in root cause analyses

Root cause analyses are only as valuable as how well they are performed. Teams often stop the analysis too early, before landing on the true root cause, resulting in recommendations that don't truly address the finding. Other times, teams can ask the right questions during the analysis but ask them only of the internal audit team or inadvertently limit interviews to individuals who only have limited knowledge of the process at hand. Organisational tone also plays a role, as companies without a culture of accountability may see root cause analyses as finger-pointing exercises instead of meaningful tools that solve problems and drive improvement.

Practical example: root cause analysis

Consider an example in which an internal audit team identifies a payment to a high-risk third party that occurred prior to the completion of the third party's due diligence review by corporate compliance. A root cause analysis using the five whys methodology is shown below.

Finding

A payment was made to a high-risk third party before corporate compliance had completed its due diligence review.

1 Why was the due diligence review incomplete at the time of payment? The third party was not one of the third parties notified for review to corporate compliance.
2 Why was the third party not in line for review? The third party was previously classified as low risk and did not require due diligence review. The company's

policy only requires due diligence review to be completed for vendors with a high-risk third-party classification as determined by its risk rating criteria; however, the third party's risk classification changed from low to high.

3 Why did the third party's risk classification change? The company's legal department amended the contract with the third party to include additional services, some of which the company considers to be high risk under its risk rating criteria for third parties; however, the compliance department was not notified of the change.

4 Why was the change in risk rating not communicated to corporate compliance? When the legal department updated the contract to include the additional services, the change was reflected in the company's contract management system, but no corresponding update was made in the company's third-party management system as updates to the contract management system do not prompt the user to update the third-party management system. When such an update is made, compliance is automatically notified of the change and requirement to complete due diligence.

5 Why was the payment processed to the third party? The company's ERP system blocks payments to high-risk third parties without a completed due diligence review based on the third party's status in the third-party management system that had not been updated.

Conclusion

In this case, the root cause is multi-faceted. A key root cause of the payment to the third party without a completed due diligence is the lack of integration between the contract management and third-party management systems and, therefore, between the legal and compliance departments. A system-generated notification from the contract management system to compliance regarding the change in the nature of services provided would resolve the issue, as would an interface between the contract management system and the third-party management system. Should the company consider this risk worth monitoring, it could develop and implement a daily, weekly or monthly monitoring protocol to identify any changes made to a third party's profile in the contract management system without a corresponding update in the third-party management system.

The interface between the ERP system and third-party management system appears to be functioning correctly; however, it is dependent on the accuracy of information within the third-party management system.

Continuous improvement

Even with proper root cause assessments and appropriate remediation plans, findings identified by auditing and monitoring exercises are significantly less powerful when examined one by one rather than aggregated and analysed at the process-wide, region-wide or organisation-wide level. Organisations that document and aggregate findings in a central repository with concrete data points that can be analysed more holistically are better positioned to track findings by topic area and root cause, to identify commonalities and trends, and to follow up on remediation plans to see whether issues were resolved.

However, no aggregation or analysis is useful if it does not reach the right audience. Often, compliance audit and monitoring findings are only raised within the compliance organisation and not with other stakeholders who have gatekeeping responsibilities, such as finance, legal (including investigations) or procurement. When those gatekeeping functions, which possess institutional knowledge and decision-making authority for the broader organisation, can see trends behind findings identified at local sites, they have better insight to enhance policies, controls, training plans and technology solutions across the organisation.

Auditing and monitoring culture

Although much of our discussion in this chapter has focused on auditing and monitoring transactions, the success of a company's compliance programme rests, in large part, on the company's culture and core values. Companies should make it a practice to embed steps within their audit and monitoring protocols to assess and document observable conduct by employees and vendors to gauge culture quality. Early detection and mitigation of organisational culture red flags, such as toxic local management, employee turnover and lack of diversity, among other things, can be exceedingly valuable in ensuring that tone at the top properly filters down throughout the organisation.

The Guide to Compliance is the first guide to tackle the compliance side of the enforcement equation in a systematic way. It combines a *tour d'horizon* of the rules in place around the world with specific practical advice for corporations and their counsel, and a scan of the horizon in parts two and three. It is part of the GIR technical library that has grown out of the *Practitioner's Guide to Global Investigations* and now includes guides to, among other things, monitorships and sanctions.

Visit globalinvestigationsreview.com
Follow @GIRalerts on Twitter
Find us on LinkedIn

ISBN 978-1-80449-257-4