REPRINT

R&C risk & compliance

BUILDING A GLOBAL COMPLIANCE & ETHICS PROGRAMME: RISK ASSESSMENT AND MONITORING

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
OCT-DEC 2019 ISSUE

www.riskandcompliancemagazine.com

Visit the website to request a free copy of the full e-magazine

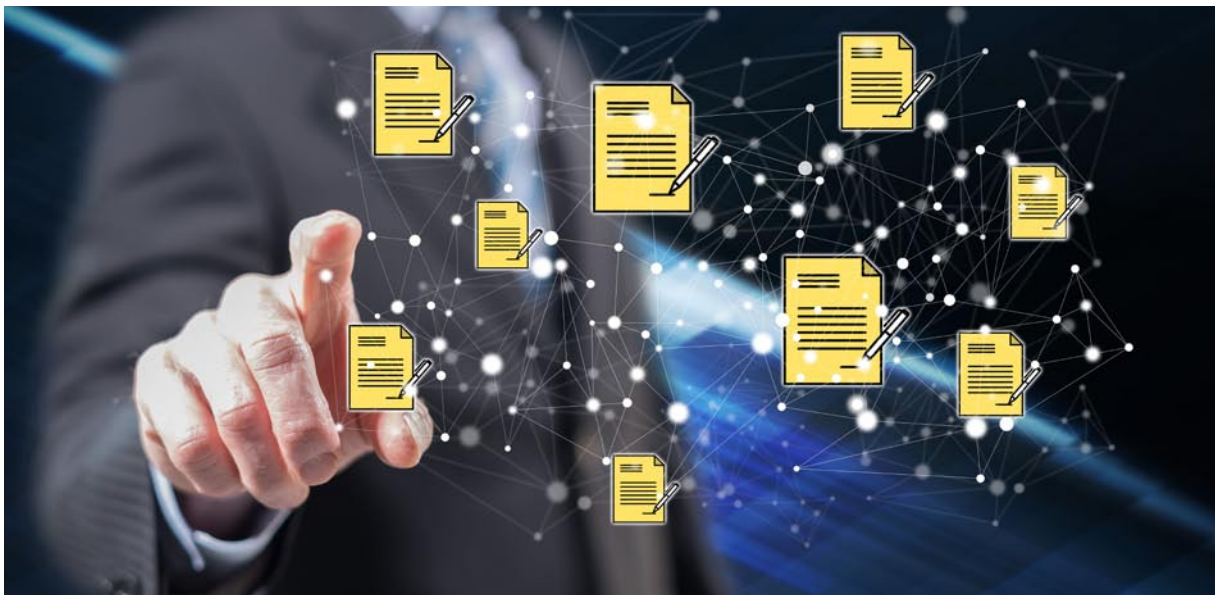
FTI CONSULTING

Published by Financier Worldwide Ltd
riskandcompliance@financierworldwide.com

www.riskandcompliancemagazine.com

EXPERT FORUM

BUILDING A GLOBAL COMPLIANCE & ETHICS PROGRAMME: RISK ASSESSMENT AND MONITORING



MODERATOR

Tapan Debnath
Senior Legal Counsel
Nokia Corporation
T: +44 (0)7342 089 528
E: tapan.debnath@nokia.com

Tapan Debnath is a specialist corporate investigation and compliance practitioner with over 15 years post qualification. He serves Nokia as head of investigations for EMEA, managing some of the company's most sensitive and high-profile matters. He is also compliance lead for a business group and is acting trade compliance counsel. Prior to Nokia, he spent five years at the UK Serious Fraud Office (SFO) investigating and prosecuting serious cases of bribery & corruption, fraud and money laundering. During this time, he was involved in developing the rules governing deferred prosecution agreements (DPAs).

PANEL EXPERTS

Andrew Durant
Senior Managing Director
FTI Consulting
T: +44 (0)20 3727 1144
E: andrew.durant@fticonsulting.com

Andrew Durant is a senior managing director in the forensic & litigation consulting segment at FTI Consulting and is based in London. He has worked in the forensic accounting sector for over 25 years and has experience across a number of industries investigating a range of issues, including financial statement fraud, stock and other asset losses, theft of confidential data, procurement and sales fraud, corruption and bribery, and investment fraud, due diligence and asset tracing assignments.

Wayne Anthony
Managing Director
FTI Consulting
T: +44 (0)20 3727 1613
E: wayne.anthony@fticonsulting.com

Wayne Anthony is a managing director in the forensic & litigation consulting segment at FTI Consulting and is based in London. He has more than 20 years of experience working in the forensic accounting field undertaking investigations, compliance reviews, financial crime investigations, asset tracing projects, litigation and dispute advisory work. His forensic accounting experience spans a wide range of industries including energy, financial services, manufacturing, pharmaceutical, publishing, engineering and charities.

Sam Eastwood
Partner
Mayer Brown
T: +44 (0)20 3130 3087
E: seastwood@mayerbrown.com

Sam Eastwood is a partner in Mayer Brown's litigation practice in London and a member of the firm's white-collar defence and compliance practice which represents corporations, boards of directors, board committees, executives and public officials in criminal, civil and regulatory enforcement proceedings around the world. He advises on ethics, anti-corruption and human rights issues in connection with companies' internal compliance policies and procedures and international business transactions. He also has significant experience in cross-border corporate investigations involving complex financial and accounting issues and anti-corruption matters throughout Africa, Asia, Europe (particularly the Nordic region), Middle East and South America.

Debnath: What are the key features of an effective company-wide compliance risk assessment programme?

Durant: The key features of an effective compliance risk programme can be classified into three main areas. First, preventing breaches by having clearly written policies and procedures, along with a strong code of conduct supported by top management, an experienced dedicated compliance officer and organisational-wide training and education adapted for local laws and regulations. The second area is detection. An effective compliance programme should have reporting hotlines readily available to all staff as well as undertaking regular monitoring and auditing of the organisation in order to detect any potential breaches or areas of high risk which need to have enhanced monitoring or updated policies and procedures. The final element is corrective action. Organisations need to ensure that if a breach has been identified they take swift and decisive action to investigate, remediate and where necessary take disciplinary action.

Eastwood: An effective compliance risk assessment requires cross-functional input beyond the compliance function and should do the following. First, identify risks resulting from violations of law, regulations, codes of conduct and other standards of practice which the company might reasonably anticipate. Second, analyse, assess and prioritise these risks. Third, evaluate the suitability and effectiveness of the company's existing controls to mitigate the identified risks. Fourth, document proposed enhancements to the company's systems and controls. Fifth, inform the extent of resources required to manage risk and the allocation of risk-related responsibilities within the company. Sixth, be approved by senior management and the board – and thereafter operate as an important management tool with regular reports on risk mitigation plans, with processes and deliverables integrated into the business calendar throughout the year. Seventh, serve as the foundation of the company's compliance programme. Eighth, be informed on an ongoing basis by the results of the company's monitoring and enforcement activity. Finally, be kept under regular review so that changes and new information can be properly assessed and reviewed on at least an annual basis.

Debnath: How does a compliance risk assessment differ from an internal audit assessment and an enterprise risk assessment? What are the interrelationships?

Eastwood: There is no one-size-fits-all approach to the allocation of risk assessment within a company. Ultimately, all relevant risk areas should be properly considered and assessed by appropriately

qualified individuals – whether such assessments are conducted by the compliance, legal, ethics, tax or human resources function is less important. The key takeaway for companies is to ensure that the responsibility for risk assessment in different risk areas is clearly documented and that each respective control function is held accountable. Senior management oversight can support in this regard. A company's compliance risk assessment, internal audit assessment and enterprise risk assessment are distinct but interrelated, interdependent and complementary. They should not be conducted in isolation of each other. All three assessment processes will necessarily address compliance risk. The enterprise risk assessment will focus on those compliance risks that significantly impact the company's ability to achieve its strategic objectives. The internal audit risk assessment is primarily focused on financial statement and internal control risk but will also address compliance risks that might materially impact the company's performance or financial statements. The compliance risk assessment will be focused entirely on compliance risk. It is important that a company's compliance risk assessment is undertaken with the benefit of relevant input from other risk assessment processes, rather than being a siloed exercise. This will ensure that the compliance-specific assessment is fully informed of developments in the company's footprint and broader strategic objectives and that it can address any relevant outcomes from internal audit reviews.

"For an organisation to determine its top compliance risks, it needs to undertake a process of identifying, collecting, measuring and assessing the full range of risks the organisation is exposed to."

Andrew Durant, FTI Consulting

Anthony: Most organisations will have an internal audit function carrying out audit risk assessments which traditionally focus on financial statement risks and other operational risks and enterprise risk assessments, to look at the risks impacting on the organisation's ability to achieve its strategic objectives. Albeit both assessments are designed to identify significant compliance-related risks, neither are specifically focused on legal or regulatory compliance risks. Although there are differences between these three risk assessments, all of which are typically owned by different functions in the organisation, there is clearly an interrelationship between them with all three's objective being to

identify and prioritise the risks the organisation faces and then assign accountability to manage and mitigate these risks.

Debnath: How should a compliance function go about identifying the top risks of the organisation?

Durant: For an organisation to determine its top compliance risks, it needs to undertake a process of identifying, collecting, measuring and assessing the full range of risks the organisation is exposed to. The process should use a combination of a framework setting out the organisation's compliance risk landscape, separating it into risk segments such as fraud and corruption, relationship with government officials or regulatory reporting, and a methodology for objectively and subjectively assessing these risks. By undertaking this process, an organisation will be able to prioritise its risks, map them to specific individuals to be accountable and allocate sufficient resources to mitigate each risk.

Eastwood: The company will have existing material – even if not a previous compliance risk assessment – which can provide an important starting point for identifying top compliance risks. This material will include enterprise risk assessments, internal audit risk assessments, internal audits, quality reviews, whistleblowing reports and investigation reports. External counsel can also assist with relevant industry benchmarking and prioritisation advice from their deep knowledge and experience of interacting with a variety of clients and regulators. Desktop research can also be informative. For example, there is plenty of publicly available guidance on the risk assessment process and competitor research can help to identify key industry risks. In addition, country profiles by institutions like the World Bank, lessons from industry scandals and reported enforcement action can be very informative. This data collection and research should then be supplemented by a combination of interviews, surveys and workshops involving a range of functions – legal, risk management, compliance, internal audit, procurement, finance and sales – as well as senior management at country, regional and local level.

Debnath: What are the legal or governance obstacles to collecting the input data? For example, for an employee survey, do local data privacy laws need to be reviewed, and workers council approvals obtained?

Eastwood: Companies are increasingly sensitive to the legal implications of collecting and processing employee data. Since the implementation of the General Data Protection Regulation (GDPR) in Europe on 25 May 2018, there has been an increased focus on data privacy considerations across organisations globally, particularly where they hold data for

European data subjects. Data privacy legislation has strengthened outside Europe as well. Accordingly, companies must take appropriate steps to ensure that all data held on company systems is collected, processed and stored in compliance with applicable data privacy laws. Where a company lacks the in-house expertise to make an assessment on data privacy risks, external specialist advice should be sought – the cost of getting it wrong, for example up to €20m or 4 percent of global turnover, whichever is higher, under the GDPR – is likely to outweigh the risk of not appropriately mitigating the risk from the outset. The particularities of local employment legislation can be an important consideration. It may be that employee surveys require the participation and approval of local workers councils, depending on how they are devised. Finally, the risk assessment process will inevitably consider, and possibly reveal, matters of some sensitivity. Companies should consider the extent to which they can and should avail themselves of the protection of legal privilege when embarking on such an exercise and regard should be had to the manner in which risks, and underlying data, are recorded and communicated.

Debnath: Should company-wide risk assessments across business segments and geographies be uniform, or should the approach be targeted and risk-specific?

Eastwood: The nature and scope of a company-wide risk assessment will depend in large part on the nature of the business itself, including the countries it operates in, the products it manufactures or the services it provides, the nature of the company's supply chain and the company's routes to market. Risk assessments should consider and assess all identified risks across all relevant business segments and geographies. However, the approach to managing those risks may vary depending on the risk assessment itself. Once risk items have been identified, the company should determine how it will allocate its resource and efforts in mitigating those risks depending on the output of its risk assessment. For large companies with varying risk profiles to consider over multiple business segments and locations, it is often simplest to adopt a broadly consistent baseline methodology for the process of identifying, analysing and addressing risks company-wide, while still allowing scope for a fit-for-purpose approach to particular business needs as required. Adopting such a consistent baseline will ensure that the company's overarching approach to managing risk can be maintained and understood as the business develops in new directions and as employees turn over.

Anthony: Compliance risks facing a global organisation are typically very complex and involve multijurisdictional laws and regulations, each having its own risk. Some compliance risks

transcend business segments or geographies, for example conflicts of interest, harassment, document management and retention. However, there are many compliance risks that are specific to an industry or business segment within a global organisation. For example, a global pharmaceutical company may manufacture in one country and distribute across many others. As a manufacturer, compliance risks such as health and safety, quality control and so on will be paramount. For the distribution entity, a key risk will be around how the sales representatives interact with government officials. Therefore, for global organisations, it is essential that their risk assessment is targeted and risk specific to the business segment or geography, but also robust, comprehensive and customisable for the different parts of the organisation.

"High quality risk assessment forms the foundation of good compliance programmes, which, in turn, shapes the culture of a company."

Sam Eastwood, Mayer Brown

Debnath: How can a compliance risk assessment support the effective allocation of resources to mitigate and manage risk?

Durant: An effective compliance risk assessment should be based on a comprehensive framework supported by an objective methodology to assess the likelihood and potential impact of each risk. This will help an organisation identify the full spectrum of the risk an organisation is exposed too. This approach will also identify the top risk priorities the organisation faces. Once identified, the organisation will be able to identify an appropriate risk owner and more importantly identify the resources required to mitigate and manage that risk. It is important that organisations regularly review their position and ensure that the allocated risk owners are suitably senior and experienced, have the required skill set and are flexible enough to be deployed efficiently to the ever-changing risks of the organisation.

Eastwood: Recommendations arising out of a compliance risk assessment should *inter alia* appropriately mitigate the identified risks, identify the responsible individuals and functions for such mitigations and set out appropriate deadlines for completing the recommended actions. Most importantly, companies should strike a balance to

ensure that the steps they take are proportionate to the corresponding risk. This is because there is no such thing as the perfect programme that is able to scrutinise every single transaction and interaction had on behalf of a company for compliance risk. In this context, the logical and defensible prioritisation of a company's resources – both employees and technology – is key to meeting regulatory expectations of an effective compliance programme. For example, Department of Justice (DOJ) guidance provides for potential credit where a company "fails to prevent an infraction in a low-risk area", if evidence is provided that an otherwise effective risk-based programme is in place, while warning against allocating a disproportionate amount of time to low-risk areas, such as modest and routine hospitality over higher risk priorities like payments to third-party consultants, suspicious trading activity or overly generous discounting practices. It is essential that key stakeholders, including senior management, and advisers are engaged with this process so that appropriate resources are allocated in order to remediate any issues accordingly.

Debnath: How would you convey to a business the benefits, financial or otherwise, of the company investing in an effective risk assessment programme?

Eastwood: It can be helpful to reflect on the impact of both external and internal stakeholders. Externally, an effective risk assessment on which robust and effective policies and procedures are based gives confidence to *inter alia* investors, shareholders, lenders, insurers, suppliers and customers that the company takes its legal and compliance obligations seriously. For a public company, this could result in enhanced share price and shareholder value. For a private company, this could be attractive to existing and potential investors. Internally, consider what kind of a culture senior management wants to engender within the company. High quality risk assessment forms the foundation of good compliance programmes, which, in turn, shapes the culture of a company. This can manifest itself in a more open work environment, higher morale among employees and more confidence among employees to speak up where issues arise. In any event, if a company can demonstrate and communicate the hallmarks of a good compliance programme, this can have a positive reputational benefit to the company, both externally and internally. In addition, emerging legislation, with a particular focus on expanding corporate criminal liability, and increased enforcement activity – particularly outside the US – are important factors. A risk assessment programme is a key foundation stone for a company's compliance programme. An effective compliance programme can reduce the incidence of misconduct within a company and can significantly mitigate the impact of any misconduct. The costs of getting compliance wrong can of course be prohibitive – in

terms of fines, lost business, debarment, litigation and then related remediation costs, in addition to reputational harm. The impact on individuals can also be very significant – fines, prison sentences and termination of employment.

Anthony: An effective compliance risk assessment supports the organisation in ensuring it operates in accordance with applicable laws and regulations wherever the organisation operates. From a purely financial perspective, any breach of law or regulation is likely to result in an investigation of the organisation both internally and by regulators. Any compliance investigation is likely to be costly, with the need for external professional advisers' support, as well as disruptive to the organisation. Any fines imposed by a regulator may also be costly – there may also be follow-on class actions. In some cases, the organisation may be banned from undertaking key activities. At worst, this could result in the collapse of the company, which will clearly impact all stakeholders, including staff. In addition, there are many other benefits, both financial and non-financial, to having an effective compliance risk assessment programme. For example, it often helps to create a 'best practice' culture of honesty and integrity which assists the organisation in meeting high ethical and professional standards to prevent frauds. This will mean that compliance issues are detected at an earlier stage and the organisation will be better positioned to take prompt corrective actions. Forewarned is forearmed.

Debnath: How can technology help compliance conduct effective compliance risk assessments in high risk areas, such as third-party sales partners and dealing with government officials?

Durant: Technology has a key role to play in assisting an organisation in manage its third-party sales partners and deal with government officials throughout the whole life cycle of the partnership – from contract negotiation, execution and contract completion. However, technology's greatest assistance is in the area of continuous monitoring and analysis of third parties and government officials throughout the life of the relationship, helping to ensure the partnership remains strong and any potential exposure to a questionable partner is detected quickly for the organisation to take corrective action. For example, technology can be used to continuously monitor media, including social media, alerting the organisation immediately to any negative publicity about its third-party sales partners or government officials it has relationships with. For large global organisations that have thousands of sales partners, technology can be used to screen large volumes of data as part of the due diligence process and can automate the annual certification of good standing process.

Eastwood: Companies are increasingly turning to artificial intelligence and automated solutions to support the day-to-day operationalisation of compliance processes, where appropriate. These solutions can enable companies to better analyse large data sets and to more efficiently identify higher risk areas, which can facilitate a company's risk management processes on a macro level. Automation helps to integrate and embed policies and procedures in a company and to improve the control environment accordingly. In the long run, automation can also help drive consistency of the application of compliance culture across a company. A more immediately apparent benefit of the increased use of technology in compliance risk assessments is that it can free up time for expert compliance personnel to conduct face-to-face meetings with third-party sale partners and training for higher risk groups internally. The use of automated solutions is often adopted as part of a company's third-party management programme to support a risk-based due diligence approach. The improvements in technology will also greatly assist internal compliance personnel's ability to effectively monitor and audit higher risk third-party relationships as part of the ongoing risk assessment process. External vendors can help a company to identify risks around third parties, such as agents and intermediaries, based on a search of online databases that indicate red flags including hits against sanctions lists, connections with politically exposed persons and news articles suggesting improper conduct on the part of that third party.

> **"Any compliance investigation is likely to be costly, with the need for external professional advisers' support, as well as disruptive to the organisation."**
>
> *Wayne Anthony, FTI Consulting*

Debnath: What is the most effective way of reporting compliance risk to a company's board, audit or risk committee?

Eastwood: The reporting of management information around compliance is a key component of ensuring that senior management have appropriate oversight of a company's compliance risk. The DOJ guidance indicates that senior management should establish "an information and reporting system in the organization reasonably designed to provide management and directors

with timely and accurate information sufficient to allow them to reach an informed decision regarding the organization's compliance with the law". The message from regulators on 'tone at the top' expectations is clear that in order to be truly engaged, senior leaders must be appropriately knowledgeable and informed on a company's evolving compliance risk profile. How such management information is delivered can vary from written board reports, to presentations to the audit committee, to discussions in board meetings. The key point is that senior management receives the information it requires in order to make a proper, informed assessment on the company's compliance with the law. The types of metrics that a company might consider reporting during a specific period includes the number of new or ongoing compliance investigations, the number of whistleblowing reports, the number of investigations that have been closed, the outcome and remediation steps in respect of closed investigations, details of lessons learned, identifying the root causes of potential misconduct, identifying and executing remediation steps to address the root causes, and the timeline and monitoring of such remediation steps. More robust analysis might consider trends of these and similar metrics over a longer period of time or across business units to provide senior management with a more in-depth understanding as to where within their company the risks lie.

Anthony: Operating in today's global business world is complex and fraught with risks and it is the responsibility of senior management to ensure these risks are mitigated. To do this, they need to have accurate, complete and timely data on the compliance risks they face, without being overloaded with information. It is therefore crucial that information to the board, audit or risk committee is communicated effectively. One of the best ways to report the key risks is via a heat map or a risk dashboard which shows the probability of a risk occurring and the potential impact on the organisation. Heat maps are a powerful way of depicting risks: they are visual, suitably concise and use colour and scaling, enabling senior management to more easily identify and focus on the risks that are most likely to occur and have the highest potential impact. R&C