REPRINT

R&C risk & compliance

ETHICS & COMPLIANCE: STANDARDS & CONTROLS

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
JAN-MAR 2020 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

EXPERT FORUM

ETHICS & COMPLIANCE: STANDARDS & CONTROLS

THE MODERATOR

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

Tapan Debnath is a seasoned corporate investigation and compliance practitioner with over 18 years' experience in criminal law, investigations and prosecution. 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 one of Nokia's major business groups and previously 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

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 18 years of experience working in the forensic accounting field undertaking fraud investigations, financial crime investigations, asset tracing projects, litigation and dispute advisory work.

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 and litigation consulting segment at FTI Consulting, and is based in London. He has worked in the forensic accounting sector for over 20 years and, in this time, he has gained experience 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. He also has extensive experience in carrying out due diligence and asset tracing assignments.

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: When developing corporate compliance policies – especially for multinational organisations – should a company strive for single, uniform global policies and standard operating procedures (SOPs)? What issues or challenges might one encounter with such an approach? When is it necessary to have local variations to policies and SOPs?

Anthony: The benefits of developing effective global corporate compliance policies that are consistent across multiple jurisdictions are often self-evident. However, it is also important to recognise that one size does not fit all and operating in certain jurisdictions brings its own unique challenges. One key area organisations need to consider when developing global operating procedures and policies is the various legal and regulatory requirements across different jurisdictions. For example, the Foreign Corrupt Practices Act (FCPA) allows for a facilitation exception, but many other anti-corruption laws, including the UK Bribery Act (UKBA), do not. Other areas for consideration are differences in cultural expectations and practices, and the dos and do nots of client entertainment is an obvious example of where caution needs to be applied. It is important for global standard operating procedures (SOPs) and polices to consider local customs and it is also essential that organisations provide proper training across all jurisdictions. Communications on global SOPs and policies could get lost in translation, so it may be difficult to ensure consistent tone at the top. Some cultures may also be less accepting of certain policies or procedures. For example, a culture that is more deferential to hierarchies may be less receptive to 'speak up' policies. Organisations need to find the balance between ensuring global SOPs and policies reflect the local legal, regulatory and cultural environment they are operating in while ensuring they are not varied to the extent that the organisation is exposed to a potential risk.

Eastwood: SOPs allow a multinational to implement international best practice consistently and create a common company culture. Challenges include delivering consistent training on SOPs, effective implementation and, at a basic level, ensuring employees are aware of where SOPs are documented. There may be a lack of 'buy-in' by local management, especially in high-risk jurisdictions where SOPs may go beyond market practice. Poorly written SOPs can lead to deviations in practice or confusion about how the SOPs should actually be implemented. SOPs may become outdated – rendering them potentially irrelevant – against evolving industry standards or business practice, which could be due to a lack of monitoring by management. Local variations may be necessary to strengthen policies and respond to identified risk in higher-risk jurisdictions – for example seeking

approval from senior management before entering into contracts with higher-risk third parties. Local variations might also be required to take into account specific standards or legislation, such as local licensing regimes, data privacy, whistleblowing, export controls or sanctions

Debnath: A common area of concern when weighing standardisation against localisation is in the concern reporting process – with some jurisdictions imposing limitations on things like anonymous reporting or reporting of certain enumerated categories of concerns. Should compliance officers be cognisant of any other areas?

Eastwood: Local laws can vary in relation to corporate political contributions, gifts and entertainment, licensing regimes in relation to sanctions and export controls and a range of other areas. State secrecy laws can be very draconian – for example, multinationals with businesses in China should ensure that they implement effective procedures and educate their employees on the risk of violating China's stringent state secrecy laws, which carry serious penalties.

Durant: Another big challenge when implementing a unified global concern reporting policy is cultural differences. For example, in the US, whistleblowers can receive large rewards and have been made the subject of Hollywood movies. However, in Germany and France there is a stigma attached to anyone considered as being an informant or a 'collaborator'.

> **"Communications on global SOPs and policies could get lost in translation, so it may be difficult to ensure consistent tone at the top."**
>
> *Wayne Anthony, FTI Consulting*

Furthermore, in some countries, such as Turkey and parts of the Middle East that have strong hierarchal structures, the concept of reporting a fellow employee – especially a member of senior management – is alien. Fear of retaliation with little or no sanctions against anyone committing the retribution is another key consideration. Again, in countries with a strong hierarchal structure and dominant management, the fear of losing your job will normally outweigh any desire to report concerns of potential wrongdoing. An effective concern-

reporting process that all employees, regardless of where they are based, can freely use with no fear of retaliation is one of the best tools in the compliance officer's armoury. This will quickly identify issues of potential wrongdoing. Compliance officers must think hard around these global differences and be prepared to adapt their global standard practices to fit their local environments – taking into account cultural differences, as well as legislative differences in order to ensure they have an effective global process in place.

Debnath: Sticking with the concern-reporting process, what are the key features of an effective concern-reporting programme in the context of an international business organisation?

Anthony: When looking at designing and implementing an effective global concern reporting programme which enables employees to share their workplace concerns safely and easily, there are several fundamental features to consider. First, clearly define the purpose of the programme. What is the ultimate aim? Second, make reporting easy and accessible to all. Ensure the reporting channels are relevant to your employees. Third, make it clear that reporting will be confidential. Wherever possible, employees should have the ability to report anonymously in order to protect their identity and reduce the fear of retaliation. Fourth, ensure there is a mechanism for reporting progress back to the employee who made the disclosure. Fifth, there should be no retaliation. Take a zero-tolerance approach and make it clear that if identified, any retaliation will be dealt with swiftly and appropriately within the laws of the jurisdiction. Finally, ensure the investigation process is transparent. Set these steps out in your policies and public notices to help build confidence that there is a defined and agreed process in dealing with reports.

> **"It should not be underestimated the amount of courage it takes for an employee to report a compliance concern to their employer. It is usually a last resort when all else fails."**
>
> *Andrew Durant, FTI Consulting*

Eastwood: Senior management should create an environment of openness where employees are encouraged to raise concerns at an early stage. In November 2018, the UK's Financial Conduct Authority (FCA) released some useful best practice, which

stated they expect boards to oversee and ensure effective whistleblowing procedures. That includes ensuring that leaders are well-equipped to respond appropriately to concerns. This preparedness arises as a result of training and documented guidance. This best practice is equally applicable beyond the financial sector. Senior management should be supported by an effective underlying infrastructure, including vigilant HR and in-house legal teams. Employees should be aware, and be trained on, the whistleblowing policy itself. The whistleblowing policy should provide an effective channel for communication, including confidential hotlines. Senior management should ensure that the policy includes a 'no retaliation' policy. It is also important to have regard to local laws and regulations – for example, Australia recently passed legislation which enhances protections available for whistleblowers, including severe penalties for breaches.

Debnath: What should companies do to encourage employees to report compliance concerns without fear of retaliation? What controls are appropriate and adequate to protect employees who have raised such concerns?

Eastwood: Senior management should encourage a culture where individuals feel comfortable raising concerns without fear of retaliation. There should be appropriate safeguards in place to protect whistleblowers, and the 'no retaliation' policy should be communicated to employees, particularly via training. When claims of retaliation are made, senior management should ensure that leaders take these claims seriously. There should be a commitment to follow-through and consequences imposed on retaliators. Investigations of retaliatory behaviours should receive special handling to ensure responsiveness and neutrality. This means that leaders across a multinational should be educated on the meaning of retaliation and should ensure that whistleblowers are monitored to check that they are not experiencing retaliation.

Durant: It should not be underestimated the amount of courage it takes for an employee to report a compliance concern to their employer. It is usually a last resort when all else fails. So, it is incumbent on the organisation to ensure that the employee can feel confident that the issues will be taken seriously without fear of retaliation. In order to encourage reporting, organisations should consider the following. First, develop and create the right environment that actively encourages employees to report concerns. Second, ensure there is a clear support from senior management; the tone from the top is vital to developing an open and ethical culture throughout the whole organisation. Third, communicate the process for raising concerns clearly to employees to increase trust and confidence regarding confidentiality. Fourth, consider publishing an anti-

retaliation policy. Fifth, to protect employees from potential retaliation, consider the use of independent third-party external reporting channels. Sixth, roll out effective training to all employees on the policies and procedures involved in reporting concerns. Finally, ensure you have the right people managing the process with sufficient seniority to make important decisions

Debnath: What controls and standards should be built into a company's investigations programme to avoid infringing data privacy and data transfer laws?

Anthony: Gathering, processing, reviewing and transferring employees' personal data in the UK has always been an issue for consideration when conducting any internal investigation, however the introduction of the EU General Data Protection Regulation (GDPR) in 2018 brought this issue to the fore. The need to investigate the actions of an employee where there are suspicions of misconduct or illegality is likely to constitute a 'legitimate interest' to access the employee's personal data. To ensure an organisation does not fall foul of the regulations, it is imperative that any investigation protocols include a clear process for evaluating the reason for accessing, using and transferring employees' personal data on a case-by-case basis. This protocol should include the following elements. First, ensure that members of the

investigation team conducting the investigation have been properly trained and are fully aware of their GDPR obligations. Second, the investigation plan must include a 'legitimate interest' assessment to justify actions, which needs to be continually reviewed throughout the investigation. Third, confirm that the processing is necessary and there is no less intrusive way to achieve the same result. Fourth, implement safeguards to reduce the impact where possible, such as restrictions on who can access the employee's personal data and with whom it may be shared. Finally, ensure working papers and electronic files that contain any employee personal data are suitably secured to protect against unauthorised access.

Eastwood: The GDPR imposes strict requirements. "Consent" to process personal data must be "freely given". Although it may be possible to rely on the 'legitimate interest' basis, this basis would need to be continually assessed. Other GDPR requirements, such as providing employees with a privacy notice to explain the legal basis of processing personal data, also highlight the importance of multinationals ensuring that procedures are in place and that staff are trained. Appropriate safeguards should be implemented to ensure that access to personal data is limited. Depending on the location of offices, policies should be tailored. Under the GDPR, data transfer to a party outside of the EU, even within a multinational, must satisfy specific conditions. Furthermore, jurisdictions such as Austria, Finland

and France are examples of jurisdictions with particularly demanding local data privacy regimes which require careful navigation.

Debnath: Given the rate at which regulatory and technological developments are impacting the design and efficiency of compliance programmes and tools, what steps should companies take to measure the overall effectiveness of compliance functions – and investigations functions in particular – and identify areas for improvement or specific regions that need special attention?

Eastwood: Senior management should systematically monitor the adequacy of compliance programmes. Regular risk assessments should be carried out to identify where new risks are emerging and the current state of compliance. The outcome of these assessments can generate 'buy-in' from senior management to allocate appropriate resources to update the compliance programme, if necessary, and address any shortcomings. Norges Bank Investment Management (NBIM), an influential investor, has recently published its anti-corruption expectations, which includes a requirement that companies should from time to time engage independent experts to review their compliance programmes. Internal audit has an important role to play in providing independent and objective assurance to the board. When considering the investigations function in particular, companies should measure the extent to which internal investigations have been successful in addressing wrongdoing.

Durant: Operating in a global business environment with constant regulatory changes means it is imperative that an organisation evaluates the effectiveness of its compliance and investigation functions. One of the best ways to do this is to conduct periodic effectiveness evaluations, which can be undertaken internally or with the assistance of external advisers. The evaluation should include the following. First, a staff survey and interviews to gauge members of the investigation team's view of how well they are doing, areas of concern and ways to improve. Second, a review of the team structure of the investigation team, including the levels, qualifications and years of experience of each member of staff, which can help identify skill gaps in specific regions. Third, a review of the current policies and procedures covering investigations to ensure they are up to date, incorporating any regulatory changes such as GDPR, changes to the organisation's structure and risk profile, applying latest technology techniques. Fourth, a detailed review of a sample of closed cases across the global organisation, from inception to final report, to identify areas of good practices and areas for improvement. Finally, where possible, benchmark the results of the evaluation against other organisations' internal investigation functions to identify potential

areas for improvement. It is also important that the results of any evaluation are reported to senior management and steps are taken to address any areas of improvement that have been identified.

Debnath: What are the key elements of conducting effective internal compliance investigations, bearing in mind that the type and seriousness of such investigations cover a wide spectrum?

Anthony: Compliance teams may get involved in a wide range of internal investigations, from employee theft through to wide-scale bribery and corruption. Irrespective of the size, scale or nature of the issue, there are several fundamental elements to conducting an effective internal compliance investigation. First, evaluate the issues and determine whether an investigation is necessary. Second, prepare a clear, detailed, written investigation plan setting out the issues to be investigated, the parties involved, the information you will require, justification for accessing employees' personal data if required and a list of potential witnesses. Third, determine the composition of the investigation team, including members of HR and legal as required, and when the investigation should be conducted. Fourth, prepare for witness interviews including ensuring all the internal HR rules have been reviewed, documented and complied with; for example, most organisations will require formal written notice to the employee or that an employee is allowed a union representative to attend, which will impact on the timing of certain interviews. Fifth, conduct interviews to gather the facts as quickly as possible, ensuring that you fully document the interview. Sixth, gather supporting documentary evidence. Seventh, evaluate the evidence. Finally, prepare a concise, detailed, fact-based objective report supported by the evidence.

> **"Internal audit has an important role to play in providing independent and objective assurance to the board."**
>
> *Sam Eastwood, Mayer Brown*

Eastwood: An organisation should support the investigative effort, including ensuring that investigators are given access to all relevant information and allocated appropriate resources, including time and money, to ensure accurate and fair results. The organisation should be transparent about

how the investigation is conducted. There should be a focus on facts and the potential causes for the incident and in turn how it could have been avoided, rather than just defending against the allegation. Regardless of the seniority of the wrongdoer, the organisation should respond with appropriate consequences.

Debnath: How should a company go about baking in good practice, such as reviewing and updating its policies, either periodically or as areas for improvement are identified?

Eastwood: An organisation should periodically review the suitability, adequacy an effectiveness of its compliance programme. However, it should also take into account relevant developments and any shortcomings that have been identified. An organisation can also engage in benchmarking against peers and best practice to identify areas for improvement and potential solutions. For example, Transparency International is developing an advanced corporate anti-corruption benchmarking offering to measure and compare the performance of anti-corruption programmes across companies.

Durant: One way to ensure compliance and investigation functions continue to improve on conducting efficient and effective investigations is to undertake periodic evaluations of the function, including a review of current policies and procedures. I would recommend that even if the organisation does not undertake a full evaluation of the function that the policies and procedures are reviewed annually by a senior member of the team and, if necessary, with the help of external advisers, to ensure they are incorporating the latest regulatory changes, such as the GDPR. Evaluation should be embedded as part of the annual review of the performance of the organisation's function, with a requirement for the heads of the relevant departments to report to the board that the review has been conducted, the results of the review and any proposed remediation. In addition, a member of the compliance function should be made responsible for ensuring teams are kept up to date with any regulatory changes, as well as changes to the organisation's structure or risk profile or new developments in investigative techniques. The individual should also be responsible for contacting the global regional heads to ascertain what is happening in local regions, which may impact global policies and procedures.

Debnath: Can there be too many compliance controls and processes which then become detrimental to the company by slowing the business down? How can the right balance be identified and achieved?

Anthony: The risks of not having sufficient, adequate and appropriate controls in place to help prevent breaches of policies, procedures or regulations are well-known. However, too many controls can have a negative impact on the business and detract from the real value of compliance. Organisations that implement unnecessary layers of controls, with check-box forms that make it difficult to run smoothly and efficiently, not only run the risk that they may lose business but that employees will try to circumnavigate these controls in order to get the job done. Identifying the right balance of controls can be very challenging in a global organisation, and it takes time and effort to really understand how different parts of the business work and where the real risks lie. This will require members of the compliance team to spend time on the front line in each region, to really understand how the business functions, major risks and what controls need to be put in place to mitigate the risk of non-compliance, without burdening the business with unnecessary controls.

Eastwood: Organisations should ensure that controls and processes are appropriate – for example, it may be a waste of resources to apply stringent due diligence on third-party agents that are 'low-risk'. Instead, organisations can identify 'workflows' which tailor the extent of certain controls and processes according to the determination of risk for a particular third-party agent. Organisations should also ensure that compliance policies are 'user-friendly' and as clear and concise as possible, so that it is easy for the business to efficiently apply procedures. When upgrading procedures, organisations should build on existing processes to facilitate compliance, rather than building from scratch.

Debnath: What emerging skills or sub-specialties do you see coming to the fore in contemporary compliance functions?

Durant: There are a number of skills that the compliance function of the future will need to ensure they remain effective, efficient and seen to be adding value. Companies need to fully embrace technology and move toward the use of artificial intelligence (AI) automation to perform advanced data analytics, providing real-time monitoring and helping identify potential compliance issues before they happen. Advances in technology, of course, also bring challenges for organisations, and compliance functions will need to be aware of increasing cyber risks and how to embed suitable controls within all aspects of the business. Compliance functions will also be under pressure to control costs – do more with less people. The successful chief compliance officer (CCO) will therefore need to be innovative in developing ways in which the compliance function will deliver efficiencies on a continual basis. R&C