ARTICLE

Looking at your compliance programme through the eyes of a prosecutor

In a roundtable discussion with Risk & Compliance magazine, FTI Consulting's Julian Glass and Katherine Gillespie and Freshfields' Ali Kirby-Harris and Ben Morgan discuss how to build a robust compliance programme.

Given recent shifts in regulatory activity and changing priorities due to the COVID-19 pandemic, to what extent has the importance of compliance programmes declined? Do companies need to guard against complacency?

Kirby-Harris: In responding to COVID-19, compliance has been just as important as ever, and has had to take account of unusual and unique risk-generating circumstances. Companies are facing novel business and financial pressure from the COVID-19 crisis which has heightened compliance risk. Experience teaches us that financial pressures from a crisis can lead to risky behaviour. Increased pressure on employees to make sales or complete contracts intensifies the risk of compliance challenges. In the context of a market downturn, there is greater risk of market manipulation and insider trading. With supply chain disruptions, companies may have to urgently find new business partners, possibly leading to reduced vetting, exposing companies to money laundering and bribery and corruption risk. In this environment, a renewed focus on robust compliance programmes is, in many cases, a business priority.

Morgan: We have seen various compliance risks emerging that are unique to the pandemic. In working from home, companies may not be working in as centralised a way as before and in some companies or industries there may be less employee visibility. Corporates will need to ensure training is fit for purpose in a remote setting and encourage employees to report potential issues even when they are not face-to-face, which can be a more challenging step to take. The shift to greater online interactions also heightens the threats posed by cyber attacks, which are even more detrimental given the dependence on digital tools. During these unique times, many corporates have rightly prioritised risks relating to the health and safety of their employees and managing the immediate risk of disruption to their businesses. However, effective compliance cannot take a back seat. Mitigating compliance risks now will help limit the disruption caused by COVID-19 in the long run, helping to ensure that the disruption is not exacerbated by investigations or litigation once we emerge from the current crisis.

Gillespie: COVID-19 has certainly changed priorities, but the importance of compliance programmes has not declined. On the contrary, compliance programmes have a key role in supporting businesses through this crisis. To address the different risks emerging in the current environment,

compliance programmes need to adapt. The most effective way to do that is to review and update compliance risk assessments, the heart of compliance programmes. Controls should be updated to mitigate the new risks identified and training should be provided throughout the organisation. Companies must safeguard against complacency as many businesses have permanently changed and their old compliance programmes may no longer mitigate organisational risks.

Glass: The pandemic should have made compliance an even greater priority, but in many cases this has not happened as companies focus on managing costs and survival. In stressful situations people make bad choices that will surface once prosecutors start to look at them. The 'fraud triangle', which is a well-known way of looking at why fraud and misconduct occurs, has three sides: pressure, opportunity and rationalisation. Pressure and opportunity have doubtless increased over the last 18 months and so misconduct will also have increased. As emergency loans start to be repaid and life starts to return to a new normal, we expect to see more cases come to light.

What guidance have regulators provided on how companies should review their own compliance programmes?

Morgan: In January 2020, the UK Serious Fraud Office (SFO) updated its Operational Handbook to include guidance on evaluating a compliance programme. It restates the Ministry of Justice's (MoJ's) six principles as guidance to assess a company's compliance programme. These include ensuring procedures are proportionate to the risk a company faces, which will require an initial risk assessment and ongoing monitoring of risk levels. The principles emphasise the importance of top-level commitment. Senior management not only have responsibility for the compliance programmes but must also foster a culture of integrity and openness. Due diligence is key to mitigating compliance risks and ensuring business relationships are transparent and ethical. Compliance programmes must be communicated effectively, through regular training, which should be monitored and evaluated to ensure it remains fit for purpose.

Gillespie: Several bodies, such as the US Department of Justice (DOJ), provide guidance for prosecutors to help them assess whether a company's compliance programme is effective. This guidance can serve as a useful lens through which companies can consider their own compliance programme. Compliance professionals can put themselves in the shoes of prosecutors. In the UK, the MoJ guidance suggests companies consider internal and external review procedures. For example, companies could consider seeking feedback from staff on the effectiveness of compliance policies and the financial control environment by using questionnaires and surveys. This feedback could also help companies understand the attitudes of staff to compliance procedures. Externally, companies could obtain best practice insights from the publications of trade bodies or regulators. Alternatively, companies may subject their existing compliance programme to external verification to obtain independent insights.

Glass: Recently there has been an increasing emphasis from prosecutors on data in compliance. There is an expectation by prosecutors that data is being used to drive compliance programmes, at the risk assessment phase, as well as for detecting violations and monitoring the programme's effectiveness. This expectation can cause problems because of the challenges of data spread across multiple systems, data privacy issues, large datasets and the structure of data not being right for use by compliance. Companies are in very different places in their journey of trying to use data to monitor and review their programmes. Some companies are at an advanced stage: they have accessed multiple large datasets, performed data cleansing, set up appropriate environments, run complicated analytics and built dashboards and visualisation tools to interpret results, whereas others are just starting to consider these requirements.

If regulators do turn their sights on a company, what are the benefits for that company if it has a robust compliance programme in place, compared to a framework that is ineffective or non-existent?

Kirby-Harris: There is a statutory defence under Section 7 of the UK Bribery Act if a company can prove it had adequate procedures in place to prevent persons associated with it from committing bribery. However, this defence has never been successfully deployed. To date, there has only been one trial in which a jury considered, and rejected, the adequate procedures defence – R v. Skansen Interiors Limited. Nevertheless, companies which have adequate procedures in place to prevent bribery and other compliance risks are in a stronger position when faced with an investigation. The ability to show a strong compliance programme will often be treated as a mitigating factor which may lead to a negotiated and more palatable resolution and can influence the severity of the terms of any such resolution. The current director of the SFO, for example, has spoken regularly about the importance of ensuring that a problem the SFO has investigated could not

happen again and appears to place as much value on that outcome as a financial penalty.

Glass: While having a strong compliance programme in place before any issue is discovered is the best position for a company to be in, it is not too late to remediate after issues have been discovered. There has been commentary from the SFO that not having a robust compliance programme might affect the amount of discount that a company receives from any penalty imposed. Given the level of penalties, this could equate to millions of pounds. The SFO is not going to let companies escape putting in place a robust compliance programme and can ask for an independent monitor or reviewer to be appointed in cases where the company has not remediated sufficiently. Therefore, it is best to remediate before a deferred prosecution agreement (DPA) to possibly reduce penalties and avoid the costs and disruption of an independent reviewer, as the programme will need to be remediated in any event.

Could you explain how regulators typically evaluate the quality of a company's compliance programme? What characteristics, processes and functions do they want to see?

Kirby-Harris: Our experience is that the SFO evaluates the quality of a company's compliance programme with direct reference to its recently published guidance. Prosecutors will assess a compliance programme both at the time of offending and in its current state. If a company has proactively strengthened its programme in light of the issues it has faced, this will be taken into consideration in the decision to prosecute and whether a DPA will be offered, and if so on what terms. It will also be considered in a prosecutor's decision on any adjustments to the level of a fine.

Morgan: In contrast to the SFO's lighter touch guidance, the DOJ's guidance provides, in detail, critical factors for evaluating a compliance programme. If a company can demonstrate the effectiveness of its compliance programme by reference to the DOJ guidelines, our view is that this is likely to have value in discussions with UK regulators and prosecutors – the SFO recognises the DOJ guidance as consistent with its own guidance. The DOJ looks at how companies' compliance programmes have evolved over time, particularly from the time of the offence to the charging decision or resolution. There is an increased emphasis on demonstrating continued and effective compliance, based on continuous risk assessment and monitoring. Another key characteristic is whether the compliance programme is adequately resourced, proportionate to the risk a company faces. Further, prosecutors want to see robust training, which among other things, ensures employees are empowered to report issues.

Gillespie: Prosecutors want to see that adequate thought has gone into the design of a compliance programme and that it is based on the specific risks of the business. One of the first things a prosecutor will look at when evaluating the adequacy of a firm's compliance programme is the risk assessment. A generic or vague programme will clearly not convince a prosecutor that a company takes compliance seriously. And it is important to demonstrate that compliance processes and procedures are kept up to date on a regular basis in response to new and changing risks, and not simply done as a one-off exercise.

Glass: In most circumstances where a prosecutor is looking at a compliance programme, something has gone wrong. The regulators will focus on the areas of failure and ask, what did your risk assessment say? Were you notified that there was an issue? What went wrong? What controls failed or what controls were missing? Typically, when looking at an issue with hindsight, there will have been red flags that should have put the company on notice that there was a risk, and this should have fed into the risk assessment. If the red flags were ignored or were not considered systemically then that becomes an aggravating factor to the prosecutor. If the risk assessment identified the risk correctly the prosecutor will then focus on any missing mitigating controls or the failure of controls that were in place. This approach does not make it easy to convince a prosecutor that a company had adequate procedures in place.

What advice would you offer to compliance professionals on ensuring their company's compliance programme stands up to regulatory scrutiny? What steps do they need to take?

Kirby-Harris: A compliance programme is never complete. It should always be evolving and responsive to changing circumstances. Those compliance programmes that function well, and add real value, have feedback loops that manage to see beyond solving an immediate problem and address the systemic and cultural triggers for that problem. As it develops, training must also be updated to reflect the current risks. Now is a good time to refresh thinking on compliance strategies. The COVID-19 crisis caused serious disruption to business practices, so companies should be considering whether the way they think about risk is as effective as it can be, now that the way we all go about our work is set to enter a new phase.

Morgan: In terms of the steps compliance professionals need to take to ensure their compliance programmes stand up to regulatory scrutiny, start with risk assessment. This is not a one-off exercise, but an ongoing monitoring obligation to ensure compliance programmes continue to be adequate and proportionate to the risk a company faces. Management must understand what the risks are and which risks have the greatest potential for damage. They should allocate resources accordingly to mitigate those risks. The SFO's expectation is that the tone is set at the top. Senior management must take active responsibility for compliance programmes, not pay lip service to it as some kind of necessary evil.

Gillespie: The most effective compliance programmes are those that have regular open communication between compliance professionals and the business. It is important to set up a compliance programme in a way that encourages open communication to gather the feedback needed to continuously improve it. For example, embedding compliance team members with certain parts of the business is vital so they can more fully understand and assess the risks. Compliance professionals need to continuously listen to and challenge the business as it helps to ensure they identify risks and bring new perspectives to strengthen the compliance programme so it stands up to regulatory scrutiny.

Glass: It is important for compliance functions to put themselves in the prosecutor's shoes and think about how they might approach any review. A useful starting point would be to address any red flags taken from whistleblower reports, investigations and internal audits or consider any sectoral issues with competitors. What do they tell you about the most pressing risks in your business? Consider these systemically rather than as standalone issues, and check that they have been fed into your risk assessment. It is also important to ensure that the risk assessment has been updated, especially for any changes in the location of the business, the type of business or the customer profiles, including, and perhaps especially, as a result of COVID-19. Ensure that all newly identified risks have been effectively mitigated and that appropriate actions have been carried out to strengthen the compliance programme. Finally, make sure the controls are operating as designed. In so many cases the issue is that controls have been bypassed, and this becomes evident as soon as anyone starts digging deeper.

This article has been reprinted with kind permission from Risk & Compliance magazine.

JULIAN GLASS
Senior Managing Director
FTI Consulting
+44 (0)75 4530 1057
julian.glass@fticonsulting.com

KATHERINE GILLESPIE
Senior Director
FTI Consulting
+44 (0)78 1183 0332
katherine.gillespie@fticonsulting.com

ALI KIRBY-HARRIS
Partner
Freshfields Bruckhaus Deringer
+44 (0)20 7716 4227
alison.kirby-harris@freshfields.com

BEN MORGAN
Partner
Freshfields Bruckhaus Deringer
+44 (0)20 7936 4000
ben.morgan@freshfields.com