

**Holly J. Gregory & Rebecca Grapsas**

Holly is a Partner and Co-Chair of the Global Corporate Governance & Executive Compensation Practice & Rebecca is Counsel in the Corporate Governance & Executive Compensation Practice, at Sidley Austin LLP



**THE CHALLENGE**  
What's missing in  
your compliance  
programme?

# Assessing corporate compliance programmes

*Assessing whether your compliance programme is 'fit for purpose' is a key element of the board's oversight responsibility*



## Corporations and their shareholders are well served in the long run by a corporate culture that emphasises compliance with the laws and regulations that the company is subject to and the ethical standards expected in the industry.

The cost of a compliance failure can be significant. Costs may result directly from penalties, settlements, legal fees, increased insurance costs, and management and board distraction. They may also result from damage to corporate reputation with its potential impact on stock price, customer and employee retention, credit ratings and the cost of capital. For these reasons, oversight of the corporation's tone at the top and the compliance programmes designed to establish and maintain that tone and detect problems is an important board responsibility.

As board and committee agendas become ever more packed, boards may find it challenging to focus on this oversight responsibility, but periodic attention to compliance matters – and, in particular, periodic assessment of whether the compliance programme is well aligned with the risks and needs of the company – remains of critical importance. This article discusses key considerations for boards in their efforts to assess whether the company's compliance programme is fit for purpose.

### Compliance: more than a paper exercise?

Corporate compliance programmes are common although there is a great deal of variation in programme size, scope, structure and resources – as well as the level of commitment from the board and senior management. It is up to each company to implement the compliance programme that best suits its needs and the level of compliance risk it is willing to take. This is a business judgment for the board as it fulfils its fiduciary responsibility to provide oversight of the compliance programme.

A company's compliance programme will fall somewhere along a continuum, with a basic effective compliance programme at the centre of the continuum, a programme that exists 'on paper' but is not effective to the left-hand side and a more robust programme to the right-hand side (see below).

When assessing the compliance programme, boards should determine where the programme currently falls on the continuum and whether adjustments

are required. In the US, boards should consider whether to undertake such an assessment now in light of new guidance from the Department of Justice (DOJ) for evaluating compliance programmes (discussed below), whether or not the company currently has any compliance issues.

### The federal compliance framework in the States

As fiduciaries, directors are required to consider the legal and regulatory compliance framework that has developed and ensure that the company has appropriate compliance-related reporting and information systems and internal controls in place. Regardless of the enforcement climate, which may or may not change under the new administration in the United States, a company and its directors, officers, employees and shareholders benefit from a corporate culture that emphasises compliance.

Each company should, at a minimum, have a basic effective compliance programme in place, i.e. a programme falling at least in the middle of the continuum described above. As well as making good business sense for a range of reasons, having an effective compliance programme can influence a federal prosecutor's decision on whether to charge

*It is up to each company to implement the compliance programme that best suits its needs and the level of compliance risk it is willing to take. This is a business judgment for the board as it fulfils its fiduciary responsibility to provide oversight of the compliance programme*

a company for the bad acts of its employees or officers and the extent to which the company may receive credit for cooperation in a settlement while helping to mitigate penalties if corporate wrongdoing is found. As recognised in the Ethics & Compliance Initiative's (ECI) recent report, *Principles & Practices of High-Quality Ethics and Compliance Program*, the de facto standard for effectiveness in compliance programme design is set out in Chapter 8 of the US Federal Sentencing Guidelines, which provides that a company must:

- Establish standards and procedures to prevent and detect criminal conduct
- Ensure board oversight of the compliance programme
- Appoint a high-level individual (such as a chief compliance officer) who has overall responsibility for the compliance programme
- Exercise due diligence to exclude unethical individuals from positions of authority

- Communicate information about the compliance programme to employees and directors
- Monitor the compliance programme's effectiveness
- Promote and consistently enforce the compliance programme
- Respond to violations and make necessary modifications to the compliance programme<sup>1</sup>

The DOJ's Principles of Federal Prosecution of Business Organizations emphasise that critical factors in evaluating a compliance programme are 'whether the programme is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the programme or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives'.<sup>2</sup>

In February 2017, the Fraud Section of the DOJ issued new guidance to provide more specific examples of how federal prosecutors will evaluate a company's compliance programme under these factors in the process of investigating and resolving an enforcement matter, while emphasising that it does not use a 'rigid formula' to make such assessments. This is the latest communication forming part of the Fraud Section's Compliance Initiative, which began with the Fraud Section's hiring of Hui Chen as full-time compliance counsel commencing November 2015. The document contains probing questions regarding the following 11 topics:

- Analysis and remediation of underlying misconduct (including prior indications)
- Senior and middle management (including conduct at the top, shared commitment and oversight)
- Autonomy and resources (including compliance function stature, experience, qualifications and empowerment)
- Policies and procedures (including gatekeepers, accessibility, operational integration, controls and vendor management)
- Risk assessment (including information gathering and analysis, and manifested risks)
- Training and communications (including availability of guidance)
- Confidential reporting and investigation (including response to investigations)
- Incentives and disciplinary measures
- Continuous improvement, periodic testing and review
- Third-party management
- Mergers and acquisitions (including due diligence process, integration in the M&A process and process connecting due diligence to implementation)

For each topic, the questions posed are designed to look behind a company's paper programme and evaluate how the programme has been implemented, updated and enforced in practice. »

Paper programme 'lip service'    Basic effective programme    More robust programme

**THE COMPLIANCE PROGRAMME CONTINUUM**

» Although some of the questions focus on the effectiveness of a company's compliance programme in the context of specific misconduct (for example, what caused the misconduct, whether there were prior indications of the misconduct and which controls failed), many of the questions focus on the compliance programme more broadly, including, for example, whether compliance personnel report directly to the board, what methodology the company uses to identify, analyse and address the risks it faces, and how the company incentivises compliance and ethical behaviour.

## Compliance programme assessments

Periodic assessment of the compliance programme, in a process overseen by the board or a board committee, helps ensure that the programme continues to be fit for purpose by identifying areas for improvement, while also creating evidence of the company's commitment to compliance for use in any future regulatory enforcement actions. Assessments should be risk-based to reflect the company's changing risk environment and to help ensure that limited compliance resources are prioritised to focus on the most significant risks.

The assessment should focus on the adequacy and effectiveness of the framework that the company has in place to fulfil the purposes of the compliance programme, which are described in the ECI Report as 'almost universal,' as follows (at 11-12):

- Ensure and sustain integrity in the company's performance and its reputation as a responsible business
- Reduce the risk of wrongdoing by the company's employees or parties aligned with the company
- Increase the likelihood that the company's management will be made aware of wrongdoing when it occurs
- Increase the likelihood that the company will responsibly handle suspected and confirmed wrongdoing
- Mitigate penalties imposed by regulatory and governmental authorities for any violations that occur

The assessment criteria should be based on the elements of an effective compliance programme outlined in federal guidance discussed above, including specific guidance from regulators regarding the company's industry. The assessment criteria should also reflect trends in settlement agreements, developing notions of recommended practices (both generally and within the company's specific industry), and the practices of peer companies, to the extent that benchmarking data is available. For example, the ECI Report discusses five core principles and supporting objectives of high-quality compliance

programmes, including examples of 'leading practices' and common pitfalls to avoid.

The focus of the board's assessment efforts should be on the company's policies, systems, incentives, and resources, as well as how senior management communicates internally about the importance of compliance. A specific area for board consideration is the extent to which the board is satisfied that the ethical tone in the company emphasises that compliance is central to strategy and therefore related to business success and priorities, and that everyone is responsible for compliance. The assessment typically relies on a combination of document review, controls and procedures testing, interviews and surveys. The board should evaluate the following and, in doing so, consider how it would answer the specific questions set forth in the DOJ's new guidance:

### *Compliance programme assessment is a key element of the board's oversight of compliance programmes*




- The board's level of oversight including availability of compliance expertise, private sessions with compliance personnel and information
- Reporting lines and related structures
- Experience, qualifications and performance of the chief compliance officer and compliance function
- Compliance function responsibilities, budget and budget allocation (including employees, outside advisors and other resources), staff turnover rate and outsourcing
- Written corporate policies and procedures regarding ethics and compliance (including legal and regulatory risks), and the process for designing, reviewing and evaluating the effectiveness of policies and procedures
- Internal controls to reduce the likelihood of improper conduct and compliance violations
- Ongoing monitoring, control testing and auditing processes to assess the effectiveness of the programme and any improper conduct

- Role of compliance in strategic and operational decisions
- Key compliance risks, risk assessment processes and risk mitigation
- Senior management conduct and commitment to compliance, and how the company monitors this
- Communication efforts by the board, CEO, other senior executives, and middle management regarding expectations and tone
- Education and training regarding compliance generally and the company's programme, policies, and procedures at all levels
- Understanding of corporate commitment to compliance at all levels
- Awareness and use of mechanisms to seek guidance and/or to report possible compliance violations, and fear of retaliation
- Specific problems that have arisen, why they arose and how they were identified and resolved
- Investigation protocols and experiences
- Performance incentives, accountability, disciplinary measures and enforcement
- Remediation and efforts to apply lessons learned

Basic compliance programmes include periodic assessments but there are questions around how often to conduct the assessment and how robust the process is. A recent PwC survey of compliance executives indicates that compliance risk assessments are typically conducted annually – 65 per cent of companies surveyed by PwC in 2016 (compared with eight per cent conducting assessments every two years).<sup>3</sup> The board will need to determine in its business judgment how often to conduct compliance programme assessments and the process for conducting assessments.

## Remaining fit for purpose

Compliance programme assessment is a key element of the board's oversight of compliance programmes. Such assessments should be conducted periodically to identify areas for improvement in light of the company's evolving risks and regulatory preferences with respect to compliance structures and practices.

The DOJ's new guidance and emerging best practice recommendations, such as those described in the ECI Report, should help boards determine the assessment process that is appropriate for the company and determine whether the company's programme continues to be effective and fit for purpose. 

<sup>1</sup>U.S. Sentencing Guidelines Manual §§ 8B2.1(b), 8C2.5(f). <sup>2</sup>DOJ, US Attorneys' Manual § 9-28.800, comment (2015) <sup>3</sup>PwC's State of Compliance Study 2016 - Chart Pack (2016) at 17.

This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and the receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers. The content therein does not reflect the views of the firm.