



© Ocean Photography/Veer

Board Assessment of Compliance Programs

In her regular column on corporate governance issues, Holly Gregory discusses the role of the board of directors in overseeing and periodically assessing the company's ethics and compliance program.



HOLLY J. GREGORY

PARTNER
SIDLEY AUSTIN LLP

Holly counsels clients on a full range of governance issues, including fiduciary duties, risk oversight, conflicts of interest, board and committee structure, board leadership structures, special committee investigations, board audits and self-evaluations, shareholder initiatives, proxy contests, relationships with shareholders and proxy advisors, compliance with legislative, regulatory, and listing rule requirements, and governance best practice.

Whether federal enforcement activity softens under the Trump administration remains to be seen, but regardless of the enforcement climate, a company and its directors, officers, employees, and shareholders benefit from a corporate culture that emphasizes compliance. A company should implement an ethics and compliance program to ensure compliance with applicable laws and regulations and ethical standards expected in the relevant industry.

The cost of a compliance failure can be significant and includes penalties, settlements, legal fees, increased insurance costs, and management and board distraction. A compliance failure can also damage a company's reputation and negatively impact its stock price, customer and employee retention, credit ratings, and cost of capital. Therefore, boards and their advisors should continue to promote an effective compliance culture and maintain processes to support that culture in the same manner as they would in a robust enforcement environment.

While compliance programs are common in companies of various sizes and types, they can differ significantly in scope, structure,

and resources, as well as in the level of commitment they receive from the board and senior management. Generally, to maintain an effective compliance program, a board should:

- Stay informed on compliance structures and practices favored by regulators, as reflected in sentencing guidelines, settlement agreements, and agency staff priorities.
- Understand emerging best practices recommendations.
- Periodically assess the compliance program in light of the company's evolving risks and identify areas for improvement. (Conducting this assessment is itself an indication that the company and the board take the compliance function seriously.)

Against this backdrop, this article explores:

- The board's fiduciary duty to oversee the company's compliance program and key issues to consider in its oversight role.
- Trends in settlement agreements, focusing on compliance reporting lines and board committees.
- The core characteristics of high-quality compliance programs, as detailed in the Ethics & Compliance Initiative's (ECI's) recent report, *Principles & Practices of High-Quality Ethics and Compliance Programs* (ECI Report) (available at ethics.org).
- Criteria for the board to assess the adequacy and effectiveness of the company's compliance framework.

THE BOARD'S OVERSIGHT ROLE

As fiduciaries, directors are charged with stewardship of the company's assets. In this capacity, directors must exercise reasonable care and good faith to ensure the company is being managed in compliance with law, regulation, and corporate policies. Over the past several decades, a series of Delaware cases, beginning with *In re Caremark International Inc. Derivative Litigation*, have emphasized that, as fiduciaries, directors must 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 (698 A.2d 959, 969-71 (Del. Ch. 1996)).

The *Caremark* case and its Delaware progeny reminded boards to pay attention to prosecutorial and sentencing guidelines and the opportunities they provide to defer prosecution and mitigate corporate and individual penalties. Compliance programs, information and reporting systems, and related controls all need to be designed in light of this framework to deter and detect compliance violations and provide senior management and the board with "timely, accurate information sufficient to allow management and the board, each within its scope, to reach informed judgments concerning both the corporation's compliance with law and its business performance." As then-Chancellor Allen observed, any "rational person attempting in good faith to meet an organizational governance responsibility would be bound to take into account" this framework "and the enhanced penalties and the opportunities for reduced sanctions that it offers." (*Caremark*, 698 A.2d at 970.)



Search [Fiduciary Duties of the Board of Directors](#) for more on directors' duties, including the duty of oversight.

THE FEDERAL COMPLIANCE FRAMEWORK

Having an effective compliance program can influence a federal prosecutor's decision whether to charge 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. For example, for cases involving Foreign Corrupt Practices Act violations, the Department of Justice (DOJ) and the Securities and Exchange Commission (SEC) "will give meaningful credit to a company that implements in good faith a comprehensive, risk-based compliance program" (DOJ & SEC, A Resource Guide to the US Foreign Corrupt Practices Act, at 59 (2012)).



Having an effective compliance program can influence a federal prosecutor's decision whether to charge 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.

The DOJ's Principles of Federal Prosecution of Business Organizations emphasize that critical factors in evaluating a compliance program are "whether the program is adequately designed for maximum effectiveness in preventing and detecting wrongdoing by employees and whether corporate management is enforcing the program or is tacitly encouraging or pressuring employees to engage in misconduct to achieve business objectives" (DOJ, US Attorneys' Manual § 9-28.800, comment (2015)).

Similarly, pursuant to the US Sentencing Commission's Federal Sentencing Guidelines, the existence of an effective compliance program can help mitigate penalties if corporate wrongdoing is found. As recognized in the ECI Report (see below *Recommendations from ECI*), the de facto standard for effectiveness in compliance program design is set out in Chapter 8 of the 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 program.

- Appoint a high-level individual (such as a chief compliance officer (CCO)) who has overall responsibility for the compliance program.
- Exercise due diligence to exclude unethical individuals from positions of authority.
- Communicate information about the compliance program to employees and directors.
- Monitor the compliance program's effectiveness.
- Promote and consistently enforce the compliance program.
- Respond to violations and make necessary modifications to the compliance program.

(US Sentencing Guidelines Manual §§ 8B2.1(b), 8C2.5(f) (US Sentencing Comm'n 2016); ECI Report, at 12.)



Search [Advantages of Implementing a Legal Compliance Program and Criminal and Civil Liability for Corporations, Officers, and Directors](#) for more on reducing liability with an effective compliance program.

INFORMATION AND REPORTING LINES

Generally, a sustained or systematic failure of the board to exercise oversight, such as a failure to ensure that a reasonable information and reporting system exists, is required to establish the lack of good faith that would be necessary to hold a director liable for a compliance failure (see *Caremark*, 698 A.2d at 970-71). A lack of good faith prevents director exculpation and indemnification under Delaware law (8 Del. C. §§ 102(b)(7), 145).

As underscored in *Caremark*, relevant and timely information is the predicate for satisfaction of the board's compliance oversight role. The board must ensure the management team designs, implements, and maintains an effective compliance program pursuant to management's delegated authority, and it should periodically assess the robustness of the compliance program and whether it is "fit for purpose." While the design of compliance programs varies significantly, key issues relate to the seniority, authority, and resources of the senior officer who is responsible for day-to-day management of the compliance function and reporting lines and practices.

SETTLEMENT TRENDS

In overseeing compliance, boards and their advisors should periodically review trends in settlements of enforcement actions, which provide insight into regulators' expectations. It is common for federal regulators to require certain compliance reporting lines and committee structures as a condition of settling an enforcement matter that implicated a compliance failure.

REPORTING LINES AND THE CCO

One regulatory concern that settlement agreements often address relates to the reporting lines for the CCO and, in particular, the relationship of the CCO to the general counsel and other senior officers. It has become common for settlement agreements to prohibit the CCO from:

- Acting in a dual role as CCO and general counsel or chief financial officer (CFO).
- Reporting to the general counsel or CFO. Instead, settlement agreements often specify that the CCO must report directly to the chief executive officer (CEO) and to the chair of the board's compliance or audit committee.
- Having responsibilities that involve acting in the capacity of legal counsel or supervising legal counsel functions for the company.

Settlement agreements typically detail the responsibilities of the CCO, for example:

- Developing and implementing policies, procedures, and practices designed to ensure compliance with the requirements of the settlement agreement and the specific regulated area in which the problem emerged.
- Monitoring day-to-day compliance activities in the area that was the subject of the enforcement action, as well as any reporting obligations created under the settlement agreement.
- Reporting on compliance matters to the board's compliance or audit committee at least quarterly.
- Chairing an internal management-level compliance committee that reports to the board or a board committee.

Settlement agreements often specify that the CCO must report directly to the chief executive officer (CEO) and to the chair of the board's compliance or audit committee.

Corporate Compliance and Ethics Toolkit

The Corporate Compliance and Ethics Toolkit available on Practical Law offers a collection of resources to assist companies in designing comprehensive internal compliance and ethics programs. It features a range of continuously maintained resources to help in-house counsel and compliance professionals understand the different laws and regulations with which a company must comply, including:

- [Corporate Governance Standards: Code of Ethics or Conduct](#)
- [DOJ and FTC Antitrust Investigations](#)
- [Foreign Corrupt Practices Act: Overview](#)
- [Handling Employment-Related Internal Investigations](#)
- [Health and Safety in the Workplace: Overview](#)
- [HIPAA Privacy Rule](#)
- [M&A Due Diligence: Assessing Compliance and Corruption Risk](#)
- [Breach Notification](#)
- [Trends in Federal White Collar Prosecution](#)
- [Responding to Equal Employment Opportunity Commission Charges](#)
- [US Securities Laws: Overview](#)
- [Whistleblower Protections Under Sarbanes-Oxley and the Dodd-Frank Act](#)

BOARD-LEVEL COMPLIANCE COMMITTEE

In addition to having a CCO, settlement agreements might require the board to assemble a compliance committee made up solely of independent directors. This committee is responsible for overseeing compliance generally and for reviewing and overseeing matters related to the area that was the subject of the settlement agreement, and it has the authority to retain, at its sole discretion, outside compliance counsel. The compliance committee also might be required to:

- Meet with the CCO in executive session (without other members of management present) at least quarterly.
- Review the compliance program, including the performance of the CCO, the management-level compliance committee, and the compliance department, at least quarterly.
- Provide the board with a report on its compliance program review.

Additionally, some settlement agreements require the board to retain an advisor to review the effectiveness of the compliance program and the related risk assessment and mitigation process. Compliance committee members might be required to adopt and individually sign resolutions for each reporting period summarizing the compliance committee's activities in reviewing and overseeing compliance in the area identified in the settlement agreement, and certifying to the compliance committee's oversight.

RECOMMENDATIONS FROM ECI

While the federal guidance regarding an effective compliance program provides a good baseline for assessing a company's compliance program, directors also should consider emerging guidance on best practices, including the ECI Report published in 2016. ECI's "Blue Ribbon Panel" of current and former CCOs (or their equivalent) from several large public companies, former enforcement officials, outside counsel, and academics prepared the ECI Report to encourage dialogue regarding effective ethics and compliance (E&C) programs.

According to the ECI Report, high-quality E&C programs share an "almost universal" purpose and certain core principles, and are distinguished by their level of effort in avoiding a "check-the-box" approach to compliance. They try to integrate compliance into the company's business operations, and they set a high priority on establishing and maintaining a culture of compliance "where concerns can be raised and where retaliation is not only prohibited but prevented." High-quality E&C programs also continually document, measure, assess, and improve on the strategies they use. (ECI Report, at 11, 15-16.)



Search [Developing a Legal Compliance Program](#) for more on implementing and maintaining an effective compliance program.

PURPOSE OF AN E&C PROGRAM

The ECI Report explains that an E&C program exists to:

- 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.

(ECI Report, at 11-12.)

PRINCIPLES OF HIGH-QUALITY E&C PROGRAMS

According to the ECI Report, high-quality E&C programs aim to establish and perpetuate "a high standard of integrity that becomes part of the DNA of the organization" and share the following five core principles:

- E&C is central to the company's business strategy.
- E&C risks are identified, owned, managed, and mitigated.

- Leaders at all levels across the company build and sustain a culture of integrity.
- The company encourages, protects, and values the reporting of concerns and suspected wrongdoing.
- The company takes action and holds itself accountable when wrongdoing occurs.

The ECI Report identifies a number of objectives that support the principles of high-quality E&C programs, and a detailed set of leading practices that contribute to each of the supporting objectives. (ECI Report, at 17-34.)

Business Strategy

The following objectives demonstrate that E&C is central to the company's business strategy:

- The E&C program is designed to integrate with business objectives.
- E&C receives the necessary resources and access to ensure both proper integration with operations and an independent voice to leaders.
- E&C personnel consistently participate in key strategic discussions.
- The company continuously improves the impact of its E&C program through leadership, innovation, and continuous feedback loops.
- The board is knowledgeable about the E&C program's impact and actively monitors its implementation across the business.
- The company shares its learning externally to positively influence other companies toward responsible practices and a commitment to integrity.

(ECI Report, at 17-21.)

E&C Risks

The following objectives support the principle that E&C risks are identified, owned, managed, and mitigated:

- The E&C program is calibrated to key risk areas identified through a robust, continuous risk assessment process.
- Leaders across the company are assigned responsibility for identifying and mitigating risks within their operations.
- The company rewards self-assessment, early issue spotting, and prompt remediation of compliance gaps.
- The company monitors as risk areas both the E&C program and the state of the company from an E&C perspective.
- Employees receive role-specific guidance and support for handling key risks.
- The company maintains rigorous third-party due diligence processes that screen for integrity.

(ECI Report, at 21-24.)

Culture of Integrity

The following objectives relate to building and sustaining a culture of integrity:

- Leaders are expected and incentivized to personally act with integrity and are held accountable if they do not.

- Leaders across the company own and are accountable for building a strong ethical culture.
- The company effectively communicates values and standards through many channels.
- All employees are supported and expected to act in line with company values and are held accountable if they do not.

(ECI Report, at 24-27.)

Reporting

The following objectives support the principle that the company encourages, protects, and values the reporting of concerns and suspected wrongdoing:

- Leaders create an environment that prepares and empowers employees to raise concerns, and provides resources to support employees in ethical decision-making.
- The company respects all employees' rights to report to government authorities.
- The company provides a broad and varied number of reporting avenues, each with effective tracking for escalation of and response to significant matters.
- The company treats all reporters the same, with consistency and fairness, throughout the process.
- The company has proactive processes in place to prevent retaliation, including:
 - awareness training for leaders;
 - monitoring of employee reporters; and
 - demonstrated consequences for violations.
- The company communicates directly with individual reporters, and more broadly with all employees, when cases are closed.

(ECI Report, at 27-31.)

Accountability

The following objectives show that the company takes action and holds itself accountable when wrongdoing occurs:

- The company regularly communicates that individuals who violate company standards or the law will be disciplined.
- The company maintains investigative excellence.
- The company consistently takes disciplinary action when violations are substantiated.
- Systems for escalation and response are well developed and regularly tested, and leaders are held accountable for compliance.
- The company makes appropriate disclosures to regulatory or other government authorities.

(ECI Report, at 31-34.)



Search [Board-Driven Internal Investigations](#) for information on key considerations and practice pointers for boards directing an internal investigation into allegations of corporate wrongdoing.

COMPLIANCE PROGRAM ASSESSMENTS

Periodic assessment of the compliance program, in a process overseen by the board or a board committee, helps identify areas for improvement while also creating evidence of the company's commitment to compliance for use in any future regulatory enforcement actions. The board's assessment should focus on the adequacy and effectiveness of the framework that the company has in place to:

- Set the tone for compliance throughout the company.
- Deter and detect compliance failures.
- Identify, manage, and mitigate compliance risks.
- Escalate issues as appropriate to the board.

As discussed above, the assessment criteria should be based on the elements of an effective compliance program outlined in federal guidance, including specific guidance from regulators regarding the company's industry. The assessment criteria also should 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 benchmarking data is available.



A specific area for board consideration is the extent to which the board is satisfied that the ethical tone in the company emphasizes that compliance is 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:

- Its level of oversight.
- Reporting lines and related structures.
- Expertise and performance of the CCO and the compliance function.

- Compliance function budget and budget allocation (including employees, outside advisors, and other resources).
- Written corporate policies and procedures regarding compliance (including legal and regulatory risks).
- Internal controls to reduce the likelihood of improper conduct and compliance violations.
- Ongoing monitoring and auditing processes to assess the effectiveness of the compliance program and any improper conduct.
- Compliance as it relates to business strategy.
- Key compliance risks, risk assessment processes, and risk mitigation.
- 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 compliance program, policies, and procedures at all levels.
- Understanding of corporate commitment to compliance at all levels.
- Awareness and use of reporting mechanisms for possible compliance violations, and fear of retaliation.
- Specific problems that have arisen and how they were identified and resolved.
- Investigation protocols and experiences.
- Performance incentives, disciplinary measures, and enforcement.
- Remediation and efforts to apply lessons learned.

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 emphasizes that compliance is related to business success and priorities, and that everyone is responsible for compliance.

The views stated above are solely attributable to Ms. Gregory and do not necessarily reflect the views of Sidley Austin LLP or its clients.