Oversight, Disclosure and Risk Management: Compliance Program Implications of Recent DOJ and SEC Actions

Published 17 March 2023 - ID G00788025 - 13 min read

Legal and Compliance Research Team

Initiatives: General Counsel, Board and C-Suite Support; Legal and Compliance Risk Management Process

Recent activity from the SEC, Delaware Chancery Court and DOJ suggest a new urgency driver for legal and compliance leaders seeking to improve their compliance program and risk management process for external reporting and officer conduct.

Background

Recent activity by the Delaware Court of Chancery, U.S. Securities and Exchange Commission (SEC) and the U.S. Department of Justice (DOJ) signal potential focus on executive risk oversight and monitoring. This puts pressure on internal and external reporting systems.

Delaware Extends Duty of Oversight to Officers

The Delaware Court of Chancery denied a motion to dismiss a derivative lawsuit against McDonald's former global chief people officer. [1] In its decision, the court, for the first time, applied the *Caremark* duty of oversight to corporate officers and held that allegations of sexual harassment can state a claim for breach of the duty of loyalty. *Caremark* and its progeny cases created an obligation for directors to implement and monitor internal control systems and address any red flags.

The court determined that because officers manage the day-to-day operations, they have a duty to identify red flags and address them or report the information to the board. The court stated that the duty of oversight is context-driven, and its application will differ depending on the role (e.g., some officers, like the CEO or CCO, will have a companywide remit, while others are limited to areas of responsibility). However, "a particularly egregious red flag might require an officer to say something even if it fell outside the officer's domain." [1]

SEC Charges Companies With Disclosure Control Violations

McDonald's

Separately, the SEC issued a cease-and-desist order charging McDonald's and its ex-CEO. [2] The SEC found that McDonald's was required to disclose all material elements of its CEO's compensation, including separation agreement terms (particularly because of the ex-CEO's misconduct). This was a novel interpretation by the SEC and could signal a change in executive compensation disclosure expectations. The SEC stated that "when corporate officers *corrupt internal processes to manage their personal reputations or line their own pockets*, they breach their fundamental duties to shareholders, who are entitled to transparency and fair dealing from executives." [3]

Activision Blizzard

Activision Blizzard settled charges with the SEC for an alleged failure to maintain internal controls designed to collect employee complaints of workplace misconduct and analyze the data for disclosure purposes. [4] The SEC found that the lack of such controls violated the requirement to maintain disclosure procedures designed to ensure information required to be disclosed was timely reported. The SEC noted that Activision Blizzard disclosed a risk factor regarding the ability to attract, retain and motivate employees. Thus, because it was aware of this risk, it should've had procedures in place to collect information relevant to assessing its disclosures. Notably, the order didn't find that the risk factor was misleading or inaccurate, or that Activision Blizzard failed to make required disclosures. This was the first time the SEC found a disclosure control violation without a corresponding disclosure violation.

DOJ Updates Guidelines on Corporate Compliance and Issues Voluntary Disclosure Policy

The DOJ issued its 2023 Guidelines on Corporate Compliance, which updated previous guidance issued in a memo by Deputy Attorney General Lisa Monaco. [5] In February 2023, the DOJ issued a Corporate Voluntary Self-Disclosure Policy, which provides incentives for voluntary corporate disclosures. [6] The DOJ noted that it considers a voluntary self-disclosure made if the company becomes aware of misconduct by employees or other agents before the information is made public and the company discloses all relevant facts prior to the threat of disclosure or voluntary investigation. Even if a voluntary self-disclosure is made, the policy outlines three aggravating factors that don't eliminate the benefits of voluntary self-reporting but do reduce them (and may require a guilty plea).

Three aggravating factors related to voluntary self-reporting are if the misconduct: [6]

1. *Poses a grave threat to national security, public health or the environment*
2. *Is deeply pervasive throughout the company*
3. *Involved current executive management of the company*

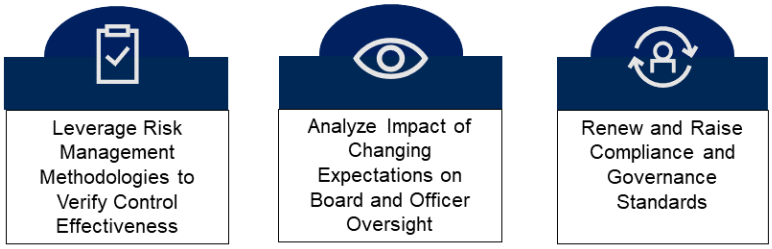
What Should Legal and Compliance Leaders Do Now?

These recent actions signal a potential heightened focus on compliance programs, risk management, and controls and procedures from both the DOJ and SEC. While the DOJ is encouraging companies to voluntarily disclose misconduct, companies can only do so if they've set up effective compliance programs, risk management strategies, and controls and procedures. Otherwise, without such self-discovery, companies risk being subject to an SEC enforcement action, and officers and directors may be subject to shareholder derivative litigation for failing to fulfill their duty of oversight.

While most organizations already have existing compliance programs, these recent actions demonstrate that programs can break down and not work as intended. Legal and compliance leaders must prioritize evaluating and modifying compliance programs, pressure-testing system operations and, together with management and the board, improving oversight processes. This will ensure they capture and elevate the right information to management and the board, take the appropriate action and maintain documentation related to these processes.

Figure 1 shows the initial three areas of focus for legal and compliance leaders.

Figure 1: Three Imperatives for Legal and Compliance Leaders



Gartner

Source: Gartner

Leverage Risk Management Methodologies to Verify Control Effectiveness

With increasing focus on reporting misconduct as soon as it's known, legal and compliance leaders should leverage existing risk management methodology from their partners in assurance (see Table 1). Enterprise risk management (ERM) and audit may have an existing methodology they can use to detect misconduct that hasn't been reported and help validate the effectiveness of controls. Further, it helps legal and compliance leaders more precisely understand the likelihood and probability of misconduct occurring depending on the data sources available. Lastly, quantitative risk management methodology can support the existing legal and compliance risk assessment process by validating assumptions.

Table 1: Five Ways Legal and Compliance Can Leverage Risk Management Methodology

(Enlarged table in Appendix)

Risk Management Methodology or Technology	Definition	Example Use Case
Real-Time Business Intelligence Reporting	Reporting and visualizations drive insights that are ingested from multiple data sources.	Use real-time reporting to triangulate information from hotline reports and employment litigation to determine the health of speak-up culture.
GRC Software for Assurance	GRC software is centered around the risk framework and control management and workflow automation for ongoing monitoring and audit.	Leverage GRC software to consolidate control testing across related global legal frameworks for TPRM.
Process Mining Technology	Process mining is designed to discover, monitor and improve real (not assumed) processes by extracting knowledge from event logs readily available in today's information systems. (For more information, see our Market Guide for Process Mining.)	Use this technology to partner with internal audit to review payment data in connection with fraud or corruption investigations.
Predictive Analysis	Processes that support predictive modeling such as regression analysis for risk management and other scenario modeling techniques can help compliance leaders understand the likelihood and probability of a risk occurring.	Use predictive modeling to help answer the question, "What is our risk exposure to noncompliance?" in any scenario where data supports the modeling. A sample scenario could include predictive risk for IP loss related to employee departure.
Algorithms, Artificial Intelligence (AI) and Machine Learning (ML)	AI, ML and algorithms can facilitate proactive monitoring of risk, enabling organizations to identify and remediate risks in near real time.	Intel's corruption risk assessment system strategically allocates resources to reduce anti-corruption risks and inform compliance audits. (For more information, see the Case Study: Adopt Incremental Corruption Risk Assessment to Efficiently Reduce Anti-Corruption Risk.)

Source: Gartner

Analyze the Impact of Changing Expectations on Board and Officer Oversight

Historically, organizations have focused on establishing sufficient board oversight processes. However, this recent activity signals that officers also must have effective oversight processes. Legal and compliance leaders should evaluate controls and procedures, clarify officers' roles and responsibilities, improve compensation structures and establish clawback policies.

Verify the Effectiveness of Information Systems

The duty of oversight requires directors *and* officers to (1) make a good faith effort to establish information systems to monitor and oversee company risks and (2) monitor those systems for indications that implicate those risks.

"Information and reporting systems exist in the organization that are reasonably designed to provide to senior management and to the board itself 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." [1]

Historically, organizations have focused on director oversight responsibility and ensuring the board is receiving the necessary information about risks to sufficiently evaluate and monitor. Now, these same types of systems must be evaluated to ensure officers also can evaluate and monitor risk by receiving necessary information and elevating issues to the board when appropriate. This doesn't require a change to the systems in place for director oversight. Instead, it means officers will need to oversee risks within their areas of responsibilities (see Table 2).

Table 2: Information Systems' Capabilities

(Enlarged table in Appendix)

Category	System Capability
Risk Management Processes	■ Educate employees about organizational risks. ■ Ensure the system captures information about organizational risks. ■ Verify that emerging risks and issues can be incorporated.
Risk Management Reporting	■ Educate employees how to report information about organizational risks. ■ Ensure the captured information is shared with officers. ■ Establish board escalation framework. ■ Verify that policies empower individual officers to bring matters to the board's attention (particularly if other officers may be implicated in information being reported).
Risk Management Documentation	■ How reported information is considered by officers when preparing public disclosures. ■ Response protocols to address issues raised. ■ Maintain records related to past and ongoing monitoring (including chain of reporting of information, how often reporting occurs and what information is reported). ■ Maintain records related to responses to any red flags or other material issues raised.

Source: Gartner

Clarify Officer Role and Responsibilities

The extension of the duty of oversight to officers amplifies the importance of officer designations. Legal and compliance leaders must consider officer designations and clearly define and document roles and responsibilities (see Table 3).

Table 3: How to Clarify Officer Role and Responsibilities

Action	How to Implement
Evaluate Criteria	Review applicable laws and regulations to determine who qualifies as an officer.
Document Role and Responsibility	Document each officer's role and responsibilities, including specific areas of oversight, and set a meeting with each officer to review role and responsibilities.
Assess Risks	Ensure each officer identifies risks within their oversight areas and documents these risks, and that the risks are evaluated as part of the organization's risk assessments and management.
Assign Risks	Ensure every material risk that is identified and disclosed has been assigned to an officer responsible for overseeing that risk and elevating any potential issues or red flags to the board.
Review Policies and Agreements	Evaluate D&O insurance policies and employment and indemnification agreements in light of officer determinations. Consider including exculpation provisions in charter.

Source: Gartner

Improve Compensation Structures and Establish Clawback Policy

DOJ prosecutors assessing an organization's compliance program will consider whether it has established a compensation structure that fosters a compliance culture and permits compensation to be recovered from individuals involved in misconduct and supervisors with knowledge, whether actually aware of the misconduct or willfully blind to it. The goal is to prevent wrongdoing before it happens and hold wrongdoers accountable.

Further, the DOJ's focus on clawback policies aligns with recent efforts by the SEC. The SEC issued rules directing securities exchanges to adopt standards requiring listed companies to establish clawback policies. This is in addition to the SEC's recent enforcement activity focusing on executive compensation matters.

In light of these developments, legal and compliance leaders should revisit current compensation structures to ensure they encourage ethical and compliance-driven behavior (see Table 4).

Table 4: Actions to Improve Compensation Practices

(Enlarged table in Appendix)

Action	Actors	How to Implement
Document Compensation Decisions	Compensation Committee Board HR Leaders	**Ensure the following actions are well-documented:** ■ How pay and performance are aligned ■ How goals or metrics are derived and what the likelihood of achievement is (i.e., are the goals or metrics so far out of reach that it could encourage risky behavior?) ■ If compensation structures of peer companies are considered in decision making ■ If and how advice provided by outside consultants, lawyers and accountants is considered ■ How compensation decisions are made upon separation (i.e., are decisions made on a case-by-case basis, or is a broader framework followed, and if any investigation is conducted to determine if there's been any misconduct)
Adopt Broad Clawback Policy	Board	**Ensure the adopted clawback policy:** ■ Provides broad discretionary authority to clawback incentive compensation in the event of misconduct or a restatement of financials due to noncompliance with financial reporting requirements ■ Establishes a framework for how misconduct is investigated and how and when a clawback decision can be made ■ Requires annual review

Consider Compliance Metrics	Compensation Committee
	Board
	HR Leaders
		Ensure the following are considered and documented:
		■ What compliance metrics the compliance leader is reporting to the board or are otherwise being considered by management
		■ What compliance metrics may be good candidates for aligning to incentive compensation to encourage good behavior
		■ How the following is communicated to employees:
		  ■ The importance of the selected compliance metrics
		  ■ The employees' role in working toward achieving those metrics

Source: Gartner

Renew and Raise Compliance and Governance Standards

The common thread between these recent newsworthy actions is that all employees, and with heightened scrutiny placed on officers, are expected to conduct themselves in accordance with company values, policies and all legal obligations. The DOJ expands upon the concept of codifying behavioral expectations with financial incentives in its updated guidance. It explicitly incorporates compliance into business outcomes by requiring prosecutors to examine "whether a company has made working on compliance a means of career advancement, offered opportunities for managers and employees to serve as a compliance 'champion' or made compliance a significant metric for management bonuses." [5]

Regular policy hygiene is an important baseline control. While 87% of compliance leaders report that they update policy and procedure in response to regulatory changes, only 16% regularly assess the effectiveness of policies and procedures. [7] Thus, compliance leaders should prioritize testing the effectiveness of policy change by measuring whether employees understand their obligations with respect to both business conduct and reporting misconduct. They should also conduct role-based refresher training with a focus on ensuring understanding by including gamification, role play and improving two-way communications in the learning process (see Table 5).

Legal and compliance leaders must continue to partner with their boards and build trust with employees by:

1. Establishing an employee value proposition for reporting

2. Reducing the risk of retaliation for raising a concern

3. Maintaining independence over and transparency into the investigation process to set the expectation that when concerns are raised, they are appropriately investigated, and discipline is consistent and fair across roles

Table 5: Role-Based Training Updates

(Enlarged table in Appendix)

Role	Training
Board Member	■ Refresher training on duty of oversight with respect to corporate compliance operations ■ Investigation training to ensure fair outcomes when concerns are raised against officers and other management-level employees
Officers	■ Duty of oversight in managing the day-to-day operations and, therefore, duty to identify red flags and address them or report the information to the board ■ The impacts of compensation as consequence management on overall compliance culture
HR and Other Employees Conducting Investigations	■ Refresher training on conducting effective investigations ■ Refresher on disciplinary procedures and company efforts to ensure a consistent approach
All Employees	■ Refresher on the value of speaking up and how to make a report of misconduct ■ Updated guidance on the investigations process, including how the company ensures consistency and provides transparency

Source: Gartner

by Alissa Lugo and Lauren Kornutick

Recommended by the Authors

Case Study: Adopt Incremental Corruption Risk Assessment to Efficiently Reduce Anti-Corruption Risk

Market Guide for Process Mining

5 Corporate Governance Trends Affecting the Board's Oversight Role in 2023

Quick Answer: How to Draft an Effective CD&A as Part of Proxy Statements

Reporting Legal and Compliance Risks to the Board

Quick Answer: How GC Can Ensure Effective Board Oversight of Risk

Evidence

[1] In re McDonald's Corporation Stockholder Derivative Litigation, U.S. SEC, C.A. No. 2021-0324-JTL (Del. Ch. January 26, 2023).

[2] In re Stephen J. Easterbrook and McDonald's Corporation, U.S. SEC, Release No. 33-11144 (January 9, 2023).

[3] SEC Charges McDonald's Former CEO for Misrepresentations About His Termination, U.S. SEC.

[4] In re Activision Blizzard, Inc., U.S. SEC, Release No. 34-96796 (February 3, 2023).

[5] Evaluation of Corporate Compliance Programs (Updated March 2023), U.S. Department of Justice, Criminal Division.

[6] Voluntary Self-Disclosure Policy (February 2023), United States Attorneys' Offices.

[7] Legal & Compliance Score for Compliance, Gartner.

Table 1: Five Ways Legal and Compliance Can Leverage Risk Management Methodology

Risk Management Methodology or Technology	Definition	Example Use Case
Real-Time Business Intelligence Reporting	Reporting and visualizations drive insights that are ingested from multiple data sources.	Use real-time reporting to triangulate information from hotline reports and employment litigation to determine the health of speak-up culture.
GRC Software for Assurance	GRC software is centered around the risk framework and control management and workflow automation for ongoing monitoring and audit.	Leverage GRC software to consolidate control testing across related global legal frameworks for TPRM.
Process Mining Technology	Process mining is designed to discover, monitor and improve real (not assumed) processes by extracting knowledge from event logs readily available in today's information systems. (For more information, see our Market Guide for Process Mining.)	Use this technology to partner with internal audit to review payment data in connection with fraud or corruption investigations.
Predictive Analysis	Processes that support predictive modeling such as regression analysis for risk management and other scenario modeling techniques can help compliance leaders understand the likelihood and probability of a risk occurring.	Use predictive modeling to help answer the question, "What is our risk exposure to noncompliance?" in any scenario where data supports the modeling. A sample scenario could include predictive risk for IP loss related to employee departure.
Algorithms, Artificial Intelligence (AI) and Machine Learning (ML)	AI, ML and algorithms can facilitate proactive monitoring of risk, enabling organizations to identify and remediate risks in near real time.	Intel's corruption risk assessment system strategically allocates resources to reduce anti-corruption risks and inform compliance audits.

(For more information, see the Case Study: Adopt Incremental Corruption Risk Assessment to Efficiently Reduce Anti-Corruption Risk.)

Source: Gartner

Table 2: Information Systems' Capabilities

Category	System Capability
Risk Management Processes	■ Educate employees about organizational risks. ■ Ensure the system captures information about organizational risks. ■ Verify that emerging risks and issues can be incorporated.
Risk Management Reporting	■ Educate employees how to report information about organizational risks. ■ Ensure the captured information is shared with officers. ■ Establish board escalation framework. ■ Verify that policies empower individual officers to bring matters to the board's attention (particularly if other officers may be implicated in information being reported).
Risk Management Documentation	■ How reported information is considered by officers when preparing public disclosures. ■ Response protocols to address issues raised. ■ Maintain records related to past and ongoing monitoring (including chain of reporting of information, how often reporting occurs and what information is reported).

- Maintain records related to responses to any red flags or other material issues raised.

Source: Gartner

Table 3: How to Clarify Officer Role and Responsibilities

Action	How to Implement
Evaluate Criteria	Review applicable laws and regulations to determine who qualifies as an officer.
Document Role and Responsibility	Document each officer's role and responsibilities, including specific areas of oversight, and set a meeting with each officer to review role and responsibilities.
Assess Risks	Ensure each officer identifies risks within their oversight areas and documents these risks, and that the risks are evaluated as part of the organization's risk assessments and management.
Assign Risks	Ensure every material risk that is identified and disclosed has been assigned to an officer responsible for overseeing that risk and elevating any potential issues or red flags to the board.
Review Policies and Agreements	Evaluate D&O insurance policies and employment and indemnification agreements in light of officer determinations. Consider including exculpation provisions in charter.

Source: Gartner

Table 4: Actions to Improve Compensation Practices

Action	Actors	How to Implement
Document Compensation Decisions	Compensation Committee Board HR Leaders	**Ensure the following actions are well-documented:** ■ How pay and performance are aligned ■ How goals or metrics are derived and what the likelihood of achievement is (i.e., are the goals or metrics so far out of reach that it could encourage risky behavior?) ■ If compensation structures of peer companies are considered in decision making ■ If and how advice provided by outside consultants, lawyers and accountants is considered ■ How compensation decisions are made upon separation (i.e., are decisions made on a case-by-case basis, or is a broader framework followed, and if any investigation is conducted to determine if there's been any misconduct)
Adopt Broad Clawback Policy	Board	**Ensure the adopted clawback policy:** ■ Provides broad discretionary authority to clawback incentive compensation in the event

		of misconduct or a restatement of financials due to noncompliance with financial reporting requirements ■ Establishes a framework for how misconduct is investigated and how and when a clawback decision can be made ■ Requires annual review
Consider Compliance Metrics	Compensation Committee Board HR Leaders	**Ensure the following are considered and documented:** ■ What compliance metrics the compliance leader is reporting to the board or are otherwise being considered by management ■ What compliance metrics may be good candidates for aligning to incentive compensation to encourage good behavior ■ How the following is communicated to employees: ■ The importance of the selected compliance metrics ■ The employees' role in working toward achieving those metrics

Source: Gartner

Table 5: Role-Based Training Updates

Role	Training
Board Member	■ Refresher training on duty of oversight with respect to corporate compliance operations ■ Investigation training to ensure fair outcomes when concerns are raised against officers and other management-level employees
Officers	■ Duty of oversight in managing the day-to-day operations and, therefore, duty to identify red flags and address them or report the information to the board ■ The impacts of compensation as consequence management on overall compliance culture
HR and Other Employees Conducting Investigations	■ Refresher training on conducting effective investigations ■ Refresher on disciplinary procedures and company efforts to ensure a consistent approach
All Employees	■ Refresher on the value of speaking up and how to make a report of misconduct

- Updated guidance on the investigations process, including how the company ensures consistency and provides transparency

Source: Gartner