R. McCONNELL GROUP PLLC

§

A BOARD GUIDE

The Compliance Legal Framework

The duties, statutes, and standards that require—and shape—an effective compliance program

Board oversight duty, securities law, Sarbanes-Oxley, the code of ethics, whistleblowing, and the program controls a company actually certifies.

2026 | R. McConnell Group PLLC

02

WHY IT MATTERS

Compliance Is a Legal Duty

A compliance program is not goodwill—it is what the law, the courts, and the markets require.

The board owes a duty of oversight.
Directors must act in good faith to ensure a reporting and monitoring system exists—and must not consciously ignore red flags.

The markets demand accuracy.
Securities law holds the company responsible for accurate, complete, and timely public disclosure.

Sarbanes-Oxley makes it concrete.
Complaint procedures, internal controls, a code of ethics, and officer certifications are statutory obligations.

A real program is a defense.
Documented controls and good-faith reliance mitigate liability; a paper program does not.

THE THROUGH-LINE

The same program elements that satisfy the board's duty are the controls the company certifies under the securities laws.

THE LANDSCAPE

03

Four Bodies of Law

Compliance sits at the intersection of corporate, securities, and statutory obligation.

FIDUCIARY & OVERSIGHT

Directors' duties of care and loyalty—and the good-faith duty to oversee risk and heed red flags.

SECURITIES LAW

Disclosure accuracy, insider-trading prohibitions, and the reporting duties of insiders.

SARBANES-OXLEY & EXCHANGE RULES

Complaint procedures, internal control over financial reporting, a code of ethics, and certifications.

WHISTLEBLOWING & PROGRAM CONTROLS

Confidential reporting, non-retaliation, and the ethics program relied on as a system of controls.

04

FIDUCIARY DUTY

The Board's Duty of Oversight

Three doctrines define what directors owe the company—and when they are protected.

Duty of Care

Act with the care a "reasonably prudent" director would use—informed of all material information reasonably available.

Duty of Loyalty & Good Faith

Act in good faith and in the company's best interests; a "systematic failure … to exercise oversight" or "conscious indifference" breaches it.

The Business Judgment Rule

Informed, good-faith decisions are presumed valid; courts will not second-guess them absent a conflict or a breach of duty.

THE OVERSIGHT PRINCIPLE

Good faith requires a board to make sure a reporting-and-monitoring system exists and to respond when it surfaces problems. The failure is not a bad decision—it is the absence of oversight, or indifference to what oversight reveals.

IN PRACTICE

05

What Active Oversight Looks Like

The duty of care is discharged through habits, not a single vote.

Stay informed

Become and remain informed about the company's operations and its industry.

Assess the key risks

Regularly assess the strategic, financial, operational, regulatory, and competitive risks the company faces.

Read before you decide

Review materials in advance, engage actively, and don't let decisions be rushed.

Reach the operators

Have access to operating levels of management and meet them to set an engaged, vigilant tone.

Keep a healthy skepticism

Challenge information and assumptions when the facts call for it.

Be vigilant with insiders

Apply extra scrutiny to matters involving company insiders.

06

SECURITIES LAW

Disclosure, Insider Trading & Section 16

Public-company status carries hard-edged duties for the company and its insiders.

Accurate disclosure

The company is responsible for accurate, complete, and timely public statements—10-K, 10-Q, proxies, and releases.

Insider trading

No trading on material nonpublic information—"material" being what a reasonable investor would consider important.

Tipping

Passing material nonpublic information to others who trade carries liability as well.

Section 16(a) reporting

Directors, officers, and large holders report their holdings and changes on Forms 3, 4, and 5.

Section 16(b) short-swing

Strict liability: profits on purchases and sales within six months are recoverable—intent is irrelevant.

Rule 10b5-1 plans

Pre-arranged trading plans, adopted in good faith with a cooling-off period, provide an affirmative defense.

07

SARBANES-OXLEY

The Statutory Spine

SOX turns good governance into specific, certifiable obligations.

§301 — Complaint procedures

The audit committee maintains confidential, anonymous channels for accounting, controls, and auditing concerns.

§404 — Internal control

Management establishes, maintains, and assesses internal control over financial reporting.

§406 — Code of ethics

A code for senior financial officers, designed to deter wrongdoing and promote honest conduct and disclosure.

§302 & §906 — Certifications

The CEO and CFO certify the reports and disclose deficiencies, material weaknesses, and fraud.

§304 — Clawback

Certain incentive pay and stock profits are recoverable after an accounting restatement.

§306 — Blackout trading

Insider trading is barred during pension-fund blackout periods.

THE CODE

08 What the Code Must Do

Statute and exchange rules dictate the floor a code of conduct must reach.

§406 — FIVE GOALS

1. Honest and ethical conduct, including handling conflicts of interest
2. Accurate public disclosure
3. Compliance with laws, rules, and regulations
4. Prompt internal reporting of violations
5. Accountability for adherence to the code

NYSE §303A.10 — SEVEN SUBJECTS

- Conflicts of interest
- Corporate opportunities
- Confidentiality
- Fair dealing
- Protection and proper use of company assets
- Compliance with laws, rules, and regulations
- Reporting of illegal or unethical behavior

SPEAK-UP

09

Whistleblowing & Non-Retaliation

The law protects the people who raise concerns—and requires the channels to do so.

Confidential, anonymous channels

SOX §301 requires procedures for confidential, anonymous submission of accounting and auditing concerns.

A duty to enable reporting

An effective program publicizes a way to report or seek guidance without fear of retaliation.

Anti-retaliation protection

SOX and the Dodd-Frank Act protect employees who report or assist from adverse action.

Audit-committee reportable criteria

Defined criteria route the most serious matters—corruption, officer misconduct, major financial integrity—to the board each quarter.

The point: a reporting system only works if people trust that raising a concern in good faith carries no penalty.

10

THE LINKAGE

The Program Is the Control

The ethics program's machinery is the very set of controls a company certifies under SOX.

Controls, not decoration

The helpline, case management, training, and the code are the controls relied upon for SOX certifications.

§404 sub-certifications

Compliance leaders sub-certify to the certifying officers that those program controls are working effectively.

Good-faith reliance

Documented sub-certifications can support the certifying officers' defense if a certification later proves inaccurate.

Change the program, change the narrative

If the program changes materially, the control narrative the company certifies must be revised to match.

11

RISK

Enterprise Risk Management

A continuous program turns the universe of risk into prioritized, owned action.

1

Identify

Surface a broad range of risks across every business segment, refreshed annually.

2

Rate

Score each risk by reputational, operational, regulatory, and financial impact, likelihood, and existing controls.

3

Mitigate

Build mitigation plans for identified gaps and assign them to executive leadership for accountability.

4

Review

Track key risk indicators; a selection of top risks is reviewed with the board at each regular meeting.

Continuous, not annual-only: risk assessment is an ongoing exercise—refreshed as new and emerging risks appear, not filed once a year.

12

FOR THE BOARD

Questions the Board Should Ask

The framework reduces to a handful of questions a director can pose directly.

1

Is there a real reporting-and-monitoring system—and do we act on what it surfaces?

The Caremark line of duty turns on a good-faith effort to oversee, and on heeding red flags.

2

Are our disclosures accurate, and are the certifications backed by tested controls?

§302/§404 certifications should rest on sub-certifications and working controls, not assurance.

3

Are the complaint channels confidential, used, and free of retaliation?

§301 procedures and anti-retaliation protection are the test of a trusted speak-up culture.

4

Does enterprise risk management drive owned mitigation—and reach this board?

Identification means little without rated risks, assigned owners, and board-level review.

Firm Lawyers

Matthew Boyden

is a trial lawyer and former federal prosecutor with more than thirty-five years of experience. He represents companies and executives in high-stakes criminal, civil, regulatory, and governance matters, and is regularly engaged where litigation risk, regulatory scrutiny, and institutional exposure intersect. His practice includes federal criminal defense, complex civil litigation, internal investigations, and board-level advisory work, including securities, sanctions and trade controls, anti-corruption, and anti-money laundering.

Larry Finder

is a trial lawyer and former United States Attorney with more than four decades of experience handling complex criminal, civil, and regulatory matters of national significance. He represents individuals, corporations, and boards confronting serious legal, institutional, and reputational risk. He served in increasingly senior roles at the U.S. Department of Justice, including Chief of the Criminal Division and First Assistant U.S. Attorney, before being appointed United States Attorney for the Southern District of Texas in 1993.

Ryan McConnell

is a former federal prosecutor and trial lawyer who represents companies, boards, and executives in high-stakes criminal, civil, and governance matters. He has tried nearly twenty federal jury trials and conducted hundreds of investigations involving complex fraud, cross-border enforcement, and sensitive regulatory issues. His practice focuses on federal criminal defense, complex civil litigation, internal investigations, and advising boards and senior executives on matters requiring judgment under pressure.