



Board Roles and Responsibilities for Fraud Risk Management

Why Boards Must Own the Risk, Not Just Hear About It

Issued by the AICPA® FLS Fraud Task Force

Lead author: **Jonathan T. Marks, CPA/CFF/CITP, CGMA, CFE, MBA, NACD Board Fellow**

The Imperative: Why Boards Must Own Fraud Risk

Across my nearly four decades of forensic investigations, one pattern recurs almost without exception. In the post-mortems that follow a major fraud, the board minutes show what the directors were told and, more significantly, what they were not told. At the moment the fraud began, those responsible for oversight believed their program was adequate. They had a hotline, a code of conduct, an internal audit function, an external auditor, and a binder somewhere that described all of it. What they did not have was a board that understood the difference between being told a program exists and knowing that the program actually works.

Summer 2026, Issue 4

Inside this issue

The Imperative.....	1
Board Responsibilities Related to Fraud and Oversight	2
The Framework: COSO's Five Principles Through the Board's Lens	4
The Candor Chain™: Why Information Erodes Before It Reaches the Board	6
Emerging Threats: AI, Cyber, and the New Fraud Landscape	7
When Oversight Fails: Lessons from the Record	8
Red Flags of Weak Board Oversight	9
Recommendations for Effective Board Oversight	11
Conclusion: From Passive Reporting to Active Oversight	12

That gap has widened over the last several years because three forces have moved simultaneously in the same direction. Regulators have raised the bar for what constitutes a credible program. Courts have narrowed the distance between passive oversight and personal liability. And the fraud itself has changed, both in who commits it and in the tools now available to commit it.

One pattern cuts through everything else. The single most common way serious fraud comes to light is a person who decides to report what they saw.¹ If tips are the leading detection method,² then the channels through which people raise concerns are not a compliance formality. They are the organization’s primary detection system.

The frauds that do the most damage are rarely the ones where no control existed. They are the ones where a control existed, and someone with enough authority went around it. That is why a board that relies solely on management reporting is structurally disadvantaged when the risk being governed is that management itself is the problem. Independent information channels are not a luxury for a board. They are the job.

Board Responsibilities Related to Fraud and Oversight

Boards are responsible for overseeing fraud risk, not managing it day to day. The chart below summarizes key responsibilities discussed in this section.

Area	Board responsibility	Key considerations
Fiduciary duties	Fulfill duties of care, loyalty, and good faith through active fraud oversight.	Seek evidence, not just assurances; understand the record being created.
Program oversight	Ensure the organization maintains a fraud risk management program that is resourced and functioning.	Ask whether the program is well designed, adequately resourced, and working in practice.
Oversight vs. management	Govern without taking on management functions.	Keep “eyes in, fingers out”: ask, challenge, verify, and document.
Independent information channels	Maintain access to information beyond management.	Use internal audit, compliance, legal, whistleblower reporting, and outside advisers.
Management override risk	Treat senior-level override as a standing fraud risk.	Ask what management can do unilaterally and who independently reviews those actions.
Audit committee authority	Use independent advisers when circumstances warrant.	Engage counsel, forensic specialists, or other experts without management approval when needed.
Considerations for smaller organizations	Adapt oversight to the organization’s resources and risk profile.	Compensate for fewer controls and limited internal audit through sharper questions and external expertise.

The single most important distinction in this entire subject is the line between oversight and management. The board oversees. Management manages. The board is responsible for ensuring that a fraud risk program exists, is resourced, works, and that the chief executive is held accountable for it. The board is not responsible for designing the controls or running the investigations. The discipline is simple: eyes in, fingers out. The board needs its eyes fully open and on the risk. It needs to keep its fingers out of the operating machinery.

¹ See the [FVS Eye on Fraud: Retaliation and Whistleblower Complaints in White-Collar Investigations](#) for detailed analysis on a forensic accountant’s perspective on organization risk, culture, and accountability (AICPA, Spring 2026 Issue).

² U.S. Securities and Exchange Commission, Office of the Whistleblower, [Annual Report to Congress for Fiscal Year 2024](#) (November 2024). The program received a record 24,980 whistleblower tips in fiscal year 2024 and awarded more than \$255 million that year; since the program’s inception in 2011, it has paid more than \$2.2 billion to whistleblowers. The volume of insider tips reflects how frequently the people closest to misconduct are the first to identify it.

There is genuine risk on both sides of that line. A board that over-delegates abdicates its duty and may learn about the fraud only after the loss. A board that over-reaches blurs accountability, entangles itself in operational decisions, and can compromise its independence at the moment independence matters most. The skill of governance is staying on the right side of that line.

A short fiduciary reminder is useful. Directors must be informed, exercise diligence, put the organization's interests ahead of personal interests, and act in good faith. The practical message is not that directors need a legal lecture. It is that a documented, functioning oversight system is now the difference between a defensible record and personal exposure.

The audit committee commonly carries primary fraud oversight, sometimes shared with a risk or finance committee, while the full board retains ultimate accountability. One feature of that structure deserves emphasis because it is so often underused: the audit committee's authority to engage independent advisers, including counsel and forensic specialists, without needing management's permission or approval. That authority exists precisely for the situation in which management is the subject of the inquiry. A board that does not know it has this power, or is reluctant to use it, has surrendered one of its most important tools.

Why Oversight Matters More in Smaller and Midsize Organizations

The oversight challenge is often more acute in smaller and midsize organizations, including private companies and not-for-profits. Smaller organizations have fewer layers of management and fewer overlapping controls, so a single point of failure has greater impact. They rely more on trust and informal processes; authority tends to concentrate in a small number of senior people; and internal audit or compliance capacity may be limited.

In that environment, oversight is often the compensating control. A board that recognizes this will govern differently. It will ask sharper questions, insist on outside expertise where internal capacity is thin, and treat its own engagement as load-bearing rather than supplementary.



The Framework: COSO's Five Principles Through the Board's Lens

When a board needs a structure for thinking about fraud risk, the most authoritative one available is the *Fraud Risk Management Guide* published by COSO.³ Its real value for a board is that it organizes the entire subject into five principles that map directly onto the five components of the COSO 2013 internal control framework. The board does not need to operate the principles. It needs to oversee them and know what good looks like for each. What follows is each principle seen from the board's chair, not the practitioner's, with the Guide's own language as the anchor.

COSO principle	COSO guidance (abbreviated)	Board responsibility	Key question directors should ask
Fraud risk governance	Establish and communicate a fraud risk management program that demonstrates the expectations and commitment of the board and senior management. ⁴	Set expectations for integrity, accountability, fraud risk governance, and oversight.	Is our fraud risk program well designed, adequately resourced, and operating effectively?
Fraud risk assessment	Perform comprehensive fraud risk assessments to identify, assess, and mitigate fraud risks. ⁵	Oversee the fraud risk assessment process and challenge its completeness.	Does the assessment include management override, cyber, AI, ESG reporting, and supply chain risks?
Fraud control activities	Select, develop, and deploy preventive and detective fraud controls. ⁶	Understand whether preventive and detective controls are operating in practice and monitor control effectiveness.	Are controls actually operating or merely documented? Who independently verifies them?
Fraud investigation and corrective action	Establish processes to obtain information about potential fraud and respond appropriately. ⁷	Ensure allegations are investigated independently and root causes are addressed.	Would employees trust our reporting process enough to raise concerns?
Fraud risk management monitoring	Perform ongoing evaluations and communicate deficiencies for corrective action. ⁸	Evaluate whether the program is tested, scored, and improved over time.	How do we know our fraud risk program is improving over time?

³ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023). The Guide is built on five fraud risk management principles corresponding to the five components of the *COSO 2013 Internal Control – Integrated Framework*. The author of this article contributed to the second edition.

⁴ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023), Principle 1: Fraud Risk Governance: "The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk."

⁵ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023), Principle 2: Fraud Risk Assessment: "The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks."

⁶ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023), Principle 3: Fraud Control Activities: "The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner." The second edition expanded its treatment of data analytics to show how analytics support each of the five principles.

⁷ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023), Principle 4: Fraud Investigation and Corrective Action: "The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner."

⁸ COSO, *Fraud Risk Management Guide, 2nd ed.* (2023), Principle 5: Fraud Risk Management Monitoring: "The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner."

Governance is where expectations are set. The program should demonstrate the board's own expectations, which means governance is not something the board reviews. It is something the board sets. The board's job is to model the conduct and the candor it wants to see, to insist that the chief executive does the same, and to make clear that results obtained by cutting corners are not results the organization will reward.

Governance also means setting fraud risk tolerance deliberately rather than by default. Every organization has a tolerance for fraud risk, whether or not it has ever discussed it. A board that has not had the conversation has simply accepted whatever tolerance happens to be embedded in current practice. Setting it on purpose, in language specific enough to guide decisions, is a governance act.

The fraud risk assessment is the most important document a fraud risk program produces, because it is the one that tells the organization where its opportunities for fraud actually are. The board does not conduct the assessment, but it should oversee its scope and challenge its completeness. A credible assessment covers the full taxonomy of fraud: fraudulent financial reporting, fraudulent nonfinancial reporting, asset misappropriation, and illegal acts such as bribery and corruption, together with the cyber-enabled schemes that now cut across all of them.

One risk must appear in every assessment as a standing item, never quietly dropped because it is uncomfortable: management override of controls. Override is the mechanism behind most of the frauds that matter to a board, precisely because it is available only to people with authority, and authority lives at the top. An assessment that does not treat override as a mandatory, ever-present risk, has skipped the very scenario most likely to produce a material loss.

For each risk identified, the assessment should identify the controls meant to address it, verify that those controls are actually implemented rather than merely described, and assess whether they are adequate to mitigate the risk. It is easy to list a control. It is harder, and far more valuable, to confirm that the control exists in operation and not just on paper. The board should also satisfy itself that the assessment reaches the emerging domains that older assessments ignore: artificial intelligence (AI); cyber; environmental and social reporting; and the supply chain. Those are not future risks. They are present ones.

A board does not need to know every control, but it should understand the architecture in broad terms. It should ask whether technology-enabled control and data analytics are actually being used to detect anomalies, and it should ask specifically about controls over management override, including manual entries, exceptions, and actions management can approve unilaterally.

What an organization does after an allegation arrives reveals more about its program than anything in its policy manual. The foundation is a reporting culture, and the practical core of that culture is a whistleblower system that people actually trust and use. When an allegation touches senior management, the audit committee should own the response in those cases, with the authority to engage independent counsel and forensic experts directly.

Corrective action closes the loop. A genuine investigation ends not with a disciplinary decision but with a root cause analysis that asks why the fraud was possible and what in the system allowed it, followed by remediation that actually addresses those causes. This is not only good practice; it is something prosecutors specifically look for.⁹

Monitoring keeps the program from decaying into a static artifact. Fraud risk should be a standing agenda item, not an occasional visitor that appears only after an incident. The board should receive periodic, independent evaluations of program effectiveness rather than self-assessments from the people who run the program. And the most useful single instrument here is an annual program effectiveness scorecard aligned to the Department of Justice's three questions: well designed, adequately resourced, works in practice.

Monitoring also means continuous improvement. Every investigation, every near miss, every control failure, and every external fraud at a comparable organization is a lesson the program should absorb. A board that asks, after each significant event, what specifically changed in the risk assessment, the controls, and the training as a result, is a board that has turned monitoring from a reporting ritual into a learning system. That is the difference between a program that ages well and one that quietly falls out of date while everyone assumes it is current.

⁹ U.S. Department of Justice, [Justice Manual § 9-47.120 \(Criminal Division Corporate Enforcement and Voluntary Self-Disclosure Policy\)](#), conditioning full remediation credit on, among other things, a demonstrated root cause analysis of the underlying conduct.

The Candor Chain™: Why Information Erodes Before It Reaches the Board

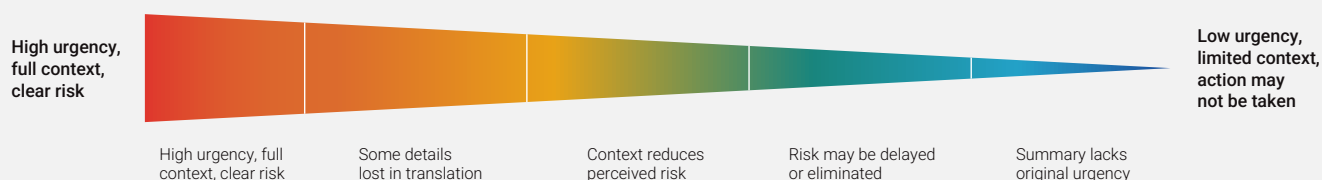
The Candor Chain™ describes the journey a piece of critical information takes from the person who first notices a problem to the board that has the authority and the duty to act on it.¹⁰ At every handoff along that journey, well-intentioned people may soften the language, add qualifiers, lead with the fix rather than the concern, or decide, sometimes without quite realizing it, that a particular detail does not need to go any higher. Each choice looks reasonable on its own. Taken together, they can turn a material red flag into a routine status update, or remove it from the conversation altogether.

How critical information loses force before it reaches the board

At each handoff, a clear warning can become softer, narrower, delayed—or stopped altogether.



Signal strength



What boards can do

- ✓ Promote a speak-up culture and protect whistleblowers
- ✓ Use independent channels to verify what you hear
- ✓ Challenge how information is framed and escalated
- ✓ Ask for both the summary and the underlying details
- ✓ Focus on what could be missing, not just what is reported

¹⁰ The Candor Chain™ is a framework developed by Jonathan T. Marks. As he defines it, the Candor Chain™ maps the journey that critical information takes as it travels from the person who first identifies a problem to the board or audit committee that has the authority and duty to act on it, and the forces that strip its urgency at each handoff. It operates through six phases, five that progressively dilute the information and one that can kill it entirely: detection, translation, contextualization, termination, aggregation, and presentation. As Marks frames the diagnostic, the question is not whether employees feel safe speaking up, but what happens to the truth after they do. See Jonathan T. Marks, *The Candor Chain™: How Information Erodes Before It Reaches the Board* (white paper, 2026); see also Jonathan T. Marks, ["The Candor Chain: What It Is and Why It Matters Now," LinkedIn](#) (2026). Candor Chain™ is a trademark of Jonathan T. Marks.

The most important point is that this is not a theory about liars. It is a theory about how organizations, staffed by honest people under real social and political pressure, can systematically produce boards that are the last to know and the first to be blamed. The question is not only whether employees feel safe speaking up. It is what happens to the truth after they do.

Breaking the chain is structural work, not cultural exhortation, and it is squarely within the board's power. The interventions are concrete. The following board best practices shorten the Candor Chain™:

- ▶ Give the board direct access to internal audit, compliance, and legal without management in the room.
- ▶ Establish skip-level reporting protocols so that information can reach the board without passing through every intermediary who might smooth it.
- ▶ Require that whistleblower metrics, including volume, themes, and outcomes, be reported directly to the relevant committee rather than summarized by management.
- ▶ Hold regular executive sessions with functional leaders below the C-suite, where the people closest to the work can speak without their superiors present.
- ▶ Periodically bring in an external adviser to assess the quality of the information flow itself, not just the information.
- ▶ Organize fraud updates around four questions:
 1. What has changed since the last update?
 2. What matters most now?
 3. What is management doing about it?
 4. Where does the board need to decide, endorse, advise, or challenge?

Emerging Threats: AI, Cyber, and the New Fraud Landscape

A fraud risk program calibrated to the threats of even five years ago is already behind. AI has arrived in fraud from two directions at once, and a board has to hold both in view. As a threat, AI has collapsed the skill required to commit sophisticated fraud: Convincing fake documents, synthetic identities, voice clones, and live deepfake video are no longer the province of specialists. The newest wrinkle is agentic AI, systems that do not merely generate content but take actions on their own, which means a scheme can now be partially automated and run at a speed and scale no human perpetrator could match. As a detection tool, the same technology offers the other side of the trade. AI and machine learning can monitor transactions continuously, surface anomalies, and flag patterns across datasets that would otherwise stay invisible.

The board's task is to make sure the organization is using AI on defense at least as seriously as adversaries are using it on offense. The Arup deepfake fraud illustrates the point.¹¹ The loss resulted from social engineering using synthetic media, not a breach of the company's information systems. Once a known executive's face and voice can be faked convincingly in real time, verification has to move out of band, to a separate channel that the impersonation cannot reach. Mandatory multichannel confirmation for high-value transfers is no longer a refinement. It is the control.

Cyber and fraud have effectively merged, and the regulatory structure now assumes it. The SEC's disclosure rules require registrants to describe the board's oversight of cyber risk in their annual reporting and to disclose material incidents on a defined timeline.¹² For boards that want a structured approach, the handbook on cyber-risk oversight produced by the National Association of Corporate Directors (NACD) with the Internet Security Alliance offers a framework built around six principles, and it has become a common reference point in boardrooms working to mature their cyber governance.¹³ A board can no longer treat cyber and fraud as separate conversations held in separate committees. A great deal of modern fraud is simply a cyber intrusion monetized.

¹¹ The fraud against the global engineering firm Arup was widely reported in 2024. A finance employee in the firm's Hong Kong office was deceived during a videoconference in which the participants he believed to be the chief financial officer and colleagues were AI-generated deepfakes. As a result, he authorized transfers totaling approximately \$25 million. The firm confirmed that its information systems were not breached; the loss resulted entirely from social engineering using synthetic media. [CNN, "British Engineering Giant Arup Revealed as \\$25 Million Deepfake Scam Victim" \(May 17, 2024\).](#)

¹² U.S. Department of Justice, Criminal Division, [Evaluation of Corporate Compliance Programs](#) (updated Sept. 23, 2024). The revision added expectations addressing the risks of AI and other emerging technologies; the use of data and data analytics within the compliance function; the proportionality of compliance resources and technology to business side investment; and the protection and encouragement of whistleblowers.

¹³ NACD and Internet Security Alliance, [Director's Handbook on Cyber-Risk Oversight](#) (5th ed., 2026), built around six cyber-risk oversight principles.

Boards should also ensure their fraud risk assessments address evolving areas such as environmental and social reporting, supply chain fraud, and digital assets. Risks in these areas range from greenwashing to falsified certifications to blockchain-related schemes that may fall outside traditional control structures. A board does not need to master any of these domains. It needs to make sure the fraud risk assessment actually reaches them, rather than stopping at the categories that were sufficient a decade ago.

When Oversight Fails: Lessons from the Record

The clearest way to see what board oversight requires is to look at what happens when it is absent. Each case is offered as a lesson about structure because in every one of them the structure is where the failure lived. They are arranged so that the classic cases establish the pattern and the more recent ones show how the law and the risk are still moving.

The first is Blue Bell Creameries, the case behind *Marchand v. Barnhill*. A listeria outbreak traced to the company's production facilities caused deaths and severe financial harm. When shareholders sued, the Delaware Supreme Court allowed the oversight claim to proceed because the board had no system for monitoring food safety, which the court treated as the most central safety and compliance issue the company faced.¹⁴ The lesson is that for a mission-critical risk, the complete absence of a board-level monitoring system is itself the breach. A board cannot oversee what it has built no mechanism to see.

The second is Boeing. After two fatal crashes of the 737 MAX, a derivative suit alleged that the board had failed to oversee aircraft safety, and the record showed there was no board committee specifically responsible for it. The case settled for \$237.5 million.¹⁵ The lesson sits one level deeper than Blue Bell. It is not enough to have a board; the board must assign clear, specific responsibility for the organization's mission-critical risks to a committee equipped to monitor them. Diffuse, unassigned oversight is functionally the same as no oversight.

The third is the most recent in legal terms and, for that reason, the one boards should study most closely. In the McDonald's derivative litigation, the Delaware Court of Chancery held for the first time that the duty of oversight, long understood to bind directors under *Caremark*, applies with equal force to corporate officers, and it allowed claims to proceed against a senior officer who allegedly ignored red flags of a culture of harassment and misconduct.¹⁶ Two features make this case worth a board's attention. First, it widened the circle of personal oversight liability beyond the boardroom to the executives the board relies on, which means the board's questions about who is accountable now have more people to land on. Second, and more important for fraud governance, the court treated conduct and culture, not just financial controls, as a proper subject of the oversight duty. That is the legal system catching up to a point this publication has been making throughout: Culture is not soft background to the real work of oversight. It is the work. A board that monitors only the numbers, and treats conduct as someone else's department, is now exposed on exactly the ground the McDonald's court found sufficient to proceed.

Fourth is FTX, the cryptocurrency exchange whose collapse in 2022 produced one of the most quoted lines in modern governance. The court-appointed executive brought in to manage the wreckage testified that he had never seen such a complete failure of corporate controls, and the founder was later convicted of fraud.¹⁷ The lesson here is FTX had almost no processes at all and a board structure that existed mainly on paper. For directors, FTX is the reminder that growth, sophistication, and market enthusiasm are not evidence of control and can actively disguise its absence. The fastest-growing, most celebrated enterprise in a sector is not exempt from the basic question this publication keeps returning to: Can anyone independent of the founder actually see what is happening, and is the board built to insist on it?

Finally, Theranos is saved for last because its lesson is the most uncomfortable for a distinguished board to hear. Theranos assembled a board of genuine luminaries, including former cabinet secretaries and senior military leaders, names that conferred enormous credibility on the company.

¹⁴ *Marchand v. Barnhill*, 212 A.3d 805, 809, 822–24 (Del. 2019).

¹⁵ *In re The Boeing Co. Derivative Litigation*, C.A. No. 2019-0907-MTZ (Del. Ch. Sept. 7, 2021).

¹⁶ *In re McDonald's Corporation Stockholder Derivative Litigation*, 289 A.3d 343 (Del. Ch. 2023). The Court of Chancery held for the first time that the *Caremark* duty of oversight extends to corporate officers, and the related opinion addressed directors' oversight of the same conduct. See also *Segway Inc. v. Cai*, C.A. No. 2022-1110-LWW (Del. Ch. Dec. 14, 2023) (confirming that the high pleading bar applies equally to officer oversight claims).

¹⁷ U.S. Department of Justice and U.S. Securities and Exchange Commission proceedings concerning FTX Trading Ltd. (2022–2024); see [DOJ sentencing release for Samuel Bankman-Fried](#) and [SEC litigation release concerning Samuel Bankman-Fried](#). The company's court-appointed chief executive testified that he had never seen "such a complete failure of corporate controls," and its founder was convicted on multiple counts of fraud and conspiracy in November 2023.

What that board lacked was anyone with the scientific or medical expertise to evaluate the blood-testing technology at the center of the enterprise, and the concerns that did surface were deflected by the founder’s charisma rather than tested by the board’s competence.¹⁸ The lesson is that prestige is not the same as oversight capacity. A board can be impressive and still be unable to ask the one question that matters, because no one in the room knows enough to know what to ask. For a *Fortune 500* board, this is the subtlest warning in the set. It is not about adding famous names or even independent ones. It is about whether the board collectively holds the specific competence to interrogate the organization’s most material risks and whether it has the skepticism to keep pressing when a charismatic executive would prefer that it stop.

The common thread across all of these case examples is not bad luck or uniquely clever fraudsters. It is governance structure, information channels, institutional skepticism, and the competence to use them. In each case, the failure was traceable to how the board was built to see, and to what it was willing to take on faith. And the more recent cases carry an additional warning: The law is steadily widening the circle of people who can be held personally accountable for failing to look.

Red Flags of Weak Board Oversight

Boards can also turn the lens on themselves. The following warning signs, drawn from extensive forensic experience, are the indicators that a board’s oversight has weakened, often without anyone intending it. They are worth reviewing candidly because most of them feel normal from the inside while they are happening.

Process red flag	Why it matters
Rubber-stamping management decisions	Management decisions are approved with little inquiry and little documentation of any challenge. The minutes record approvals but not questions.
Late and rushed agendas	A growing share of time-sensitive or significant items arrives late, leaving no real opportunity for the board to study them before deciding.
Retroactive approvals	The board is asked to ratify decisions management has already made and acted on, converting oversight into after-the-fact endorsement.
Unclear or manipulable metrics	The measures management reports are vague, inconsistent, or constructed in ways that can be adjusted to produce a desired result.
Thin financial information	The board receives less financial detail than its responsibilities require, and requests for more are met with friction or delay.
Missing financial expertise	The board lacks members with the accounting and finance background needed to interrogate what management presents.
Limited auditor interaction	The board lacks direct access to internal or external auditors outside management.
Management-supplied justifications	The rationale for significant actions is consistently framed by management in a way that places the burden of disagreement on the board.
Chronic delay of information	Key financial information and responses to board requests are continually postponed, so the board is always working from a stale picture.

Any one of these can have an innocent explanation. The concern is the pattern. A board that recognizes several of these suggests oversight is quietly giving way to ratification.

The red flags above are largely about process, the mechanics of how information reaches the board. There is a second set that operates at a deeper level, about leadership character and board behavior. Directors who recognize them early, and who act rather than explain them away, can stop the compounding before it becomes catastrophic.

¹⁸ John Carreyrou, *Bad Blood: Secrets and Lies in a Silicon Valley Startup* (New York: Alfred A. Knopf, 2018); see also contemporaneous reporting that the Theranos board comprised prominent former government and military officials but few members with the scientific or medical expertise relevant to the company’s blood-testing technology. Elizabeth Holmes was convicted of fraud in 2022.

Behavioral red flag	Why it matters
The bigger-than-life CEO or chair	Hubris clouds judgment, and the seeds of destruction are often sown in the best of times, when success breeds overconfidence and criticism is dismissed as jealousy. A board has to keep its independent perspective precisely when the organization appears to be thriving.
Unmanaged conflicts of interest	Conflicts should be eliminated or fully disclosed at once. When they are tolerated, minimized, or hidden, they corrupt decision-making and open pathways for misconduct.
Over-specialized board silos	When directors focus narrowly on their own committee without understanding the broader enterprise, the connections between risks go unnoticed. The audit committee may see financial irregularities while the compensation committee sees aggressive targets, and no one connects the two.
Excessive pressure and leveraged compensation	When reward depends heavily on hitting specific metrics, the temptation to bend rules intensifies. A board has to balance motivation against the recognition that excessive pressure is itself a fraud risk.
Intense institutional loyalty	Loyalty that distorts transparency causes people to defer to leaders even when they are wrong. In a healthy organization, loyalty runs to the mission and the values, not to individuals, and the moment questioning leadership becomes disloyal, critical information stops flowing.
CEO personal misconduct	Character in personal matters often predicts character in professional ones. A board should not wave away warning signs simply because they arise outside the workplace.
Failure to speak truth to power	When an atmosphere of fear and silence masks trouble, the organization loses its early warning system. Directors should probe actively for signs that subordinates are afraid to raise concerns, and they should build direct channels for unfiltered information.
Directors as caretakers rather than owners	When directors treat their role as passive oversight rather than active ownership, engagement declines. A board that sees itself as merely approving management's recommendations will not exercise the independent judgment that fiduciary duty requires.



Recommendations for Effective Board Oversight

Diagnosis is only useful if it leads to action. The following recommendations distill what separates boards that genuinely own fraud risk from boards that merely receive reports about it. They are deliberately practical, and they are within the reach of any board willing to use the authority it already has.

- ▶ **Conduct independent compensation reviews.**
Examine executive compensation and incentive structures without management running the process, because incentives are where pressure is manufactured and where the conditions for fraud are often built.
- ▶ **Require comprehensive annual risk assessments.**
Insist on a fraud risk assessment that is genuinely annual, genuinely comprehensive, and explicitly reaches the rapidly evolving domains of AI; cyber; environmental and social reporting; privacy; and the supply chain.
- ▶ **Obtain outside board training.** Bring in independent education on directors' roles and responsibilities, on how fraud actually works, and on the evolving legal standards, rather than relying on internal briefings that may carry the organization's own blind spots.
- ▶ **Maintain clear, regularly reviewed policies.** Keep board policies and procedures current, review them on a defined cycle, and make sure they reflect the organization as it is now, not as it was when the policies were written.
- ▶ **Ask questions and request supporting documentation.**
Make it routine to question management and to request selected supporting documentation, not because the board distrusts management, but because verification is the substance of oversight.

- ▶ **Insist on timely action and follow-up.** Track issues to resolution with named owners and dates, so that identified problems are actually closed rather than noted and forgotten.
- ▶ **Demand clear, effective reporting of concerns.**
Make certain the whistleblower hotline and ethics reporting channels are trusted, accessible, and reported on directly to the board, because they are the organization's leading detection system, not a compliance formality.

Beyond these governance practices, there is a category of independent forensic advisory work that boards increasingly find valuable precisely because it sits outside the management reporting line. This is practitioner work, distinct from the board's own oversight work, and the distinction matters: The board governs, while the practitioner provides the board with independent capabilities it does not have in-house. That advisory work includes Candor Chain™ diagnostic assessments that evaluate how well information actually moves to the board; fraud risk management program scorecards built on the Department of Justice's three questions; education for directors on AI-enabled fraud risk specifically; and help designing the board-level fraud risk reporting that gives directors a clear, undistorted line of sight into the program. Used well, these are not a substitute for the board's judgment. They are a way of equipping the board to exercise it.

Finally, the most useful instrument a board has is a set of honest questions it asks of itself, before a crisis forces them. The following are not abstract governance prompts. They are the questions that, asked earlier, tend to change the afternoon in the audit committee room when bad news finally arrives. They are meant to be revisited, not answered once and filed.

- ▶ **On the quality of information:** Do I receive the information I need to fulfill my oversight responsibilities, or am I relying primarily on what management chooses to share? Have I ever been surprised by bad news that others in the organization already knew, and if so, what kept it from reaching me sooner?
- ▶ **On culture and transparency:** What happened to the last person who brought bad news, was that outcome visible to others, and what message did it send?
- ▶ **On risk oversight:** What are the mission-critical risks for this organization, and am I receiving direct, unfiltered information about them? What are we not discussing that we should be? What assumptions underlie our strategy, and how would we know if they were wrong?
- ▶ **On horizon intelligence:** Does the organization have a structured, documented process for identifying emerging risks before they surface as internal red flags? When the world changes between board meetings, what is the protocol for getting updated intelligence to the board before the next scheduled one?
- ▶ **On personal judgment:** Am I applying appropriate skepticism, or do I default to trust? Am I willing to be the dissenting voice when necessary, or do I defer to preserve collegiality?
- ▶ **And most important of all:** What information was identified but never reached me?

Conclusion: From Passive Reporting to Active Oversight

The difference between the boards that get blindsided by fraud and the boards that catch it early is rarely intelligence, diligence, or good intentions. The difference is structural. It is whether the board built itself to see.

Owning fraud risk is not about receiving more reports. A board can drown in reports and still be the last to know. It is about changing how the board works: keeping eyes in and fingers out, building independent channels that let the truth reach the table, testing whether the program works in practice, and documenting the work before the loss rather than after it.

The good news is that the core tools are already within the board's power. The authority to engage independent advisers; meet with internal audit, compliance, and legal without management; require a real fraud risk assessment; demand a scorecard; and insist on decision-useful reporting already exists. What is required is not new power. It is the will to use the power the board already holds, deliberately and on a schedule. That is what it means to own fraud risk. The board that does it will not eliminate fraud because no one can. But it will be the board that sees, the board that acts, and the board that can show, when the hard questions come, that it did the work.





aicpa-cima.com

© 2026 Association of International Certified Professional Accountants. All rights reserved. AICPA and CIMA are trademarks of the American Institute of CPAs and The Chartered Institute of Management Accountants, respectively, and are registered in the US, the EU, the UK and other countries. The Globe Design is a trademark of the Association of International Certified Professional Accountants.

For information about obtaining permission to use this material other than for personal use, please email copyright@aicpa-cima.com. All other rights are hereby expressly reserved. The information provided in this publication is general and may not apply in a specific situation. Legal advice should always be sought before taking any legal action based on the information provided. Although the information provided is believed to be correct as of the publication date, be advised that this is a developing area. The Association, AICPA, and CIMA cannot accept responsibility for the consequences of its use for other purposes or other contexts.

The information and any opinions expressed in this material do not represent official pronouncements of or on behalf of the AICPA, CIMA, or the Association of International Certified Professional Accountants. This material is offered with the understanding that it does not constitute legal, accounting, or other professional services or advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

The information contained herein is provided to assist the reader in developing a general understanding of the topics discussed but no attempt has been made to cover the subjects or issues exhaustively. While every attempt to verify the timeliness and accuracy of the information herein as of the date of issuance has been made, no guarantee is or can be given regarding the applicability of the information found within to any given set of facts and circumstances.

2607-956308