2023

Combating corporate reporting fraud: learnings from leading European audit committee chairs

tapestry NETWORKS

EY Building a better working world

A large-scale fraud can not only wreak havoc on the company directly affected, but it can also erode trust in capital markets. Recent high-profile frauds have led stakeholders to ask how Europe's largest companies can do more to prevent, detect, and mitigate fraud.

Fraud risk oversight is a persistent concern for audit committees. From 2020 to 2022, Tapestry Networks, with the support of EY, conducted in-depth conversations with experienced audit chairs as part of a multiphased research project to explore how audit committees can strengthen governance in this area. This paper presents our cumulative findings, emphasizing practical recommendations for audit committees. Every board and company are different, and we expect that readers will adapt practices to their particular situations, in consultation with professional advisers.

For a list of reflection questions for audit committees, please see Appendix 1. For details of the research process and a list of participating audit chairs, please see Appendix 2.

Our research identified the core issue facing audit committees today: fraud risk is constantly evolving, and qualitative aspects, such as culture and cognitive biases, create unique oversight challenges.

Participants identified six approaches that can help address the challenges and complexity of fraud risk:

- **Define roles and responsibilities within the financial reporting ecosystem**
- **Acknowledge and address corporate culture challenges and cognitive biases**
- **Establish clear processes and cultural expectations around whistleblower and speak-up programs**
- **Use technology to help combat fraud**
- **Prepare for emerging fraud risks associated with ESG data and reporting**
- **Increase audit committee and board education on fraud risk**

Fraud risk oversight is complex and challenging

Fraud comes in many forms, both financial and nonfinancial, including theft, tax fraud, bribery, collusion, distortion of information (financial and regulatory), and data theft and manipulation. This project focused on financial fraud but covers some aspects of nonfinancial fraud where, in the words of one audit chair, *"it impairs the view of the shareholders regarding the sustainability of the business."* [1]

Although corporate reporting fraud is hardly new, overseeing it remains a challenging and complex task for audit committees. Participants explained why:

- **The nature of fraud risk, like cyber risk, is constantly evolving.** *"Fraud is an unknown unknown,"* a participant noted. *"You keep attacking it, but the nonobvious fraud is the most difficult."* Major frauds occur infrequently, and detecting rare events that are designed to be concealed is difficult and expensive. Audit chairs *"have to keep a risk-reward lens"* when determining how to allocate resources, one advised.

- **Collusive fraud is particularly challenging to uncover.** Certain recent major frauds in Europe have involved collusion among senior executives, making them hard to detect. One participant said, *"If a fraud is very complex, it would be very tricky for internal auditors, external auditors, the audit committee, or board to spot it without inside intelligence."* Another said, *"Fraud is extremely hard to identify when you're dealing with top management manipulation."* Such frauds can elude even the best control systems.

- **Corporate culture, a critical indicator of fraud risk, is difficult to assess.** Audit chairs repeatedly said that corporate culture was the single most important factor related to combating fraud. *"It always goes back to culture,"* one stressed. Culture, including tone at the top, impacts both the likelihood of fraud and the willingness of employees to report issues. But getting an accurate read on culture can be difficult for boards. *"How can we come closer to understanding the culture part, which is a huge risk?"* one audit chair asked. A speak-up culture can be difficult to assess or build.

> "It always goes back to culture.
> —Audit Chair"

- **The three lines of defense can be weakened by cognitive biases.** Participants pointed out that groupthink, confirmation bias, optimism bias, and the effect of charismatic leaders can influence how groups receive and process information. These biases can obscure signs of a potential fraud.

- **Whistleblower systems can be compromised.** *"One of the most important ways to discover fraud is through whistleblower systems. Most of what we detect comes through those systems,"* one audit chair stated. But implementing a *broad "speak-up"* culture in a global company can be tricky. Employees who spot bad behavior may keep quiet if they fear that speaking up will put them at risk of retaliation or if they lack trust in leadership's willingness to take action. In certain countries, cultural norms may inhibit reporting peers or superiors. Regulatory environments also play a role. For example, regulations in Europe provide fewer protections and incentives for whistleblowers than those in the United States.[2]

- **Technologies to prevent and detect fraud are advancing but are not sufficient on their own.** Audit chairs recognize the significant capabilities that technologies like machine learning and artificial intelligence (AI) bring to identifying outliers and trends that signal fraud risk; however, most audit committees are still learning how these technologies work. *"You don't want to be dependent on something you don't understand,"* one audit chair remarked. Mike Savage, a global forensic and integrity services leader at EY, noted that even as technology becomes increasingly able to detect potential fraud and risk of fraud, audit committees *"should not depend on one algorithm to be the silver bullet."* Using multiple tools and methods to analyze fraud risk, including human judgment, is key.

- **Fraud risk reports vary in effectiveness, and audit chairs grapple with what data to ask for and how to interpret it.** While some audit chairs are satisfied with the data they receive related to fraud risk, others said that trying to draw conclusions from it can be challenging. For instance, whistleblower tips may be significantly higher in a specific region or period, and although an uptick in reporting could signal greater fraud risk, it could also merely indicate increased trust in the whistleblower process. One audit chair reported, *"Following some changes in compliance and legal staff, we saw an increase in whistleblower hotline inbounds. What we're trying to understand is should we attribute it to a positive culture change and increased trust? Or is it something else?"*
- **Environmental, social, and governance (ESG) reporting creates new fraud risks.** As companies integrate ESG initiatives into their core business and align their results with profitability, the potential for fraud arises. Many audit committee chairs are less aware of ESG fraud than they are of financial fraud and consequently may not take the proactive steps needed to prepare for this emerging risk. *"This is something I'm quite worried about,"* one said. *"I don't know if we're doing what we should. It is new territory."*
- **Fraud-specific education or training for audit committees and boards is rare.** Audit committee members often receive training on topics such as third-party risk or cybersecurity, but most have not had training specifically focused on fraud. Participants agreed that this could be beneficial. Fraud risk oversight is a complex task, and the best way to learn is often through case studies or real-life examples, they said. *"You may read something in another case and realize that you need to go back and address it better at your company,"* one noted. Aside from reviewing examples, members were unsure how to provide helpful training opportunities related to fraud.

Define roles and responsibilities within the financial reporting ecosystem

Stakeholders in a company's reporting system—the board, management, internal audit, external auditors, and the audit committee—all have a common interest in an ethical culture and a control environment that inhibits fraud. Audit chairs agreed that management and internal audit teams retain primary responsibility for fraud detection and prevention. And they believed that external auditors are functioning in an adequate and appropriately limited role. But participants stressed the need for clarity around the roles and responsibilities of each function, which many described as not clearly defined within their companies. Audit chairs emphasized that boards and audit committees need constant vigilance and strong cooperation from all financial reporting participants:

- **Management** serves as a company's first line of defense against fraud. But participants pointed out that audit committees must balance maintaining a trusted relationship with management with a skeptical mindset in assessing fraud risk. They highlighted the importance of making sure that management teams view fraud as a high-priority risk. *"Everyone thinks it won't happen to them ... or the immediate tendency is to say it is a one-*

off issue, not systemic," one said. Audit chairs should help management teams recognize that fraud is a risk for all companies and should engage management on how they are prioritizing and emphasizing their role in fighting it. One member cautioned, *"You don't want management to feel targeted."* But for collusive frauds in particular, audit committees must make *"a judgment of key people ... You don't want to be skeptical the whole time because you need to partner and work with management, but once a year, you may need to step back and create time for skepticism."*

- **The CEO**, in particular, has a unique influence on a company's approach to fraud. One audit chair recommended having a conversation with the *CEO "to understand how they view their role in communicating about fraud and the tone the company sets for addressing reports of fraud."* Tolerance for slipshod behavior or a lack of interest in the topic may be a red flag. Boards should also be aware of CEOs *"sugar coating"* information when problems arise. As appropriate, audit committees should consider seeking input from the *"next level of management [in] conversations without others present."*
- **Internal audit (IA)** is the second line of defense, and audit chairs described the IA team as their *"eyes and ears within the company."* Audit committees should ensure that *"fraud is high enough on the yearly internal audit plan,"* participants said. Audit chairs stressed the importance of balancing risk prioritization with attention to the basics. Most said their IA teams use a risk-based approach to prioritize where teams spend time and resources related to fraud prevention and detection, but *"the challenge with a risk-based approach is that the areas which would fall under traditional financial fraud are not always considered high risk."* One audit chair asks IA to include a section on fraud risk in every report to keep it top of mind throughout the year.
    - **Build agility into IA teams.** Flexible capacity is key, an audit chair said: *"Internal audit is the single biggest tool we have when something is off. We changed our approach this year and have built 10% of our audit capacity as spare so we can do targeted work when and where it's needed. It was particularly useful during COVID."*
    - **Ensure IA teams are sufficiently trained and diverse.** *"Internal audit was historically focused on financial audits, but their remit is now much broader and looks at all the risks in a business,"* an audit chair said. This requires more extensive and diverse skill sets. Audit committees should ensure that IA teams learn how to adopt a supportive, but skeptical approach, enlisting additional expertise as needed—for example, hiring data forensic experts. Audit chairs also flagged diversity as vital, especially for global companies: *"All of our audit teams are diverse in international background, experience, knowledge, and gender. We are completely convinced that if you want a successful approach in internal audit, you need a diverse team."*
- **External auditors** also play an important role. While fraud is not the primary focus of external auditors, international standards state that auditors are responsible for obtaining "reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error."[3] Participants acknowledged that

there are inherent limitations in the external auditors' ability to detect material fraud. But some felt that auditors and audit committees could work together to further enhance a focus on combating fraud. They shared the following suggestions:

> ***It's important for an audit chair to build a relationship with the external auditors. They need to trust that I will be careful with how I use what I hear, and vice versa.***
>
> *—Audit Chair*

- **Prioritize transparency and trust between the external auditor and audit committee.** Open, candid dialogue with the external auditor is crucial, audit chairs said. But external auditors are *"not always prepared to be very transparent with the audit chair and can sometimes hesitate to mention issues,"* one said. *"It can take time to build trust,"* but doing so should be a priority. *"It's important for an audit chair to build a relationship with the external auditors. They need to trust that I will be careful with how I use what I hear, and vice versa."*
- **Use private sessions to gain insight on potential issues.** External auditors have unique views and perceptions of the factors shaping the ethical culture of the company, and they *"spend a lot more time in the business than I do,"* an audit chair said. Holding regular private sessions with the external auditor can be valuable. *"I have private conversations—just myself and the auditor. We regularly catch up and share questions, concerns, and views that might be hard to articulate on paper. It's an important part of the cultural assessment,"* a participant said.
- **Develop relationships throughout the external audit team.** While audit chairs typically interact primarily with the lead audit partner, engaging with other members of the external audit team can help audit chairs reinforce tone at the top and emphasize fraud prevention and detection as a priority. *"I might start asking to meet with a wider group of the audit team to encourage a speak-up culture,"* one participant said. Another described a practice that worked well: *"Once a year, we had all worldwide partners involved in the audit get together for lunch, which was very useful and allowed me to engage with local partners."*
- **Ask external auditors to monitor external information sources, such as short-seller reports, social media, and press.** In the case of Wirecard, the German company that collapsed in 2020 after the discovery of a major fraud, the groups that successfully raised red flags were journalists, short sellers, and whistleblowers.[4] This demonstrated that external information sources can function as an early-warning signal for potential fraud. Recognizing the role that third parties may play in fraud detection, EY has established a center to provide ongoing monitoring of short-seller reports, social media, and other external information sources to inform risk assessments and fraud-related procedures. Audit chairs agreed that monitoring external sources is a good practice.

Acknowledge and address corporate culture challenges and cognitive biases

Audit chairs consistently cite corporate culture as a key factor in enabling or inhibiting fraud. They often speak of the importance of tone at the top. But a large company may have hundreds of thousands of employees in countries around the world, and an audit committee may struggle to assess culture both as a whole and in specific regions or business units. Audit chairs discussed a variety of methods to evaluate culture, including culture audits and direct employee feedback from engagement surveys or whistleblower tips. They also provided suggestions to help audit committees glean insights about culture in other ways:

- **Dig into how employees interpret tone at the top and assess "mood in the middle."** Participants said that senior leaders should both relay appropriate tone from the top and follow up with employees to assess how messages are received as they are *"cascaded down."* Additionally, determining whether cultural expectations permeate the *"mood in the middle"*—i.e., mid-level management and employees charged with implementing policies and processes—is important to understand how culture varies within the company. Participants reported using trainings and surveys to monitor how employees interpret culture and converting survey data into actionable information to coach and direct CEOs and CFOs. Audit committees can also perform site visits: *"I think that's the true place to get under the skin of a company. I visited some entities to get insight into how they're thinking, what they're saying, and if they actually use the same words as the senior management company."*
- **Ask for real-time reports on culture and behavioral trends.** Having internal audit teams speak up quickly if something feels out of line can provide crucial insight, participants said, even if the matter does not require a formal, written report: *"I rely a lot on internal audit to get a grasp of culture issues. If you develop a trustworthy relationship, you get a lot of value and insight."* Together with human resources (HR), internal audit has valuable insight into behaviors *"from sloppy to devious"* that could signal fraud risk, an audit chair noted. One described how internal audit teams often *"know things 'between the lines' that they cannot qualify."* This audit chair said internal audit was asked *"to create a side report with unqualified issues,"* which enables the audit committee to determine if issues need more attention.
- **Include comprehensive analyses of culture in fraud risk assessments.** *"Organizational culture is one of the major influencers of speak-up behavior in a company,"* Katharina Weghmann, global ESG forensics leader at EY, explained, *"so audit committees should be mindful of how culture either contributes to or inhibits speak-up behavior and be sensitive to early-warning signals and trends."*

"**Audit committees should be mindful of how culture either contributes to or inhibits speak-up behavior and be sensitive to early-warning signals and trends.**"

—Katharina Weghmann, EY Global ESG Forensics Leader

Using data to help decode culture

Incorporating a broad range of tools and metrics, such as those below, can help audit committees understand culture as a potential signal of fraud risk.

- Employee surveys
- Culture audits
- Whistleblower hotline reports
- Site visits
- Exit interviews
- HR data such as staff tenure, absenteeism, turnover, and promotion rates
- Compensation and incentives data
- Internal audit reports – formal and informal
- External auditor feedback – formal and informal
- External information, e.g., short-seller reports and social media

Participants noted that increasingly, audit committees and boards need to expand the type of data they review to get a clearer view of culture. Audit committees are approaching this in a variety of ways, as summarized in the table to the left. Data from HR can be especially insightful. *"We are looking at data and trends that you wouldn't necessarily think are useful, but that indicate patterns, such as staff tenure, how frequently people have moved around, and whether they take their annual leave. It is enabling us to consider what additional forensic work may be needed by internal audit,"* one participant reported. Another suggested that proposed promotions be cross-checked against whistleblower data, internal audit reports, and other HR data.

For additional Tapestry material on board oversight of culture, see our Ethics, Culture, and Compliance Network's **Assessing Corporate Culture: A Practical Guide to Improving Board Oversight** *and the European Audit Committee Leadership Network's* **Oversight of Corporate Culture**.

Establish clear processes and cultural expectations around whistleblower and speak-up programs

Whistleblower systems and speak-up hotlines and cultures are critical to maintaining trust and accountability. Audit chairs identified well-functioning whistleblower systems as a central tool in combating fraud. A 2022 report by the Association of Certified Fraud Examiners (ACFE) on frauds committed by individuals against their companies reinforces this view. In its study of more than 2,000 fraud cases across 133 countries and 23 industries, ACFE found that companies with whistleblower hotlines detected fraud more quickly and experienced smaller financial losses than companies without them.[5] It also found that 42% of fraud cases were uncovered by whistleblower tips—nearly three times the level as internal audit, the next most common fraud detection method.[6] Participants described practices that enhance oversight and cultural expectations related to whistleblower systems and speak-up cultures:

- **Having clear governance structures that promote trust in the process.** The most important practice, audit chairs said, is having a structure that promotes trust among employees, establishes confidential reporting mechanisms, protects whistleblowers, and demonstrates that internal reporting leads to action. In some companies, hotline reports go directly to the audit chair, while in others they go to another board committee. In others, hotline reports go to a group outside of the company; some audit chairs believe that this encourages use of the system by reinforcing its confidentiality. Audit committees should examine whether their current structure to receive tips and complaints promotes trust in the reporting process.

- **Regularly reviewing whistleblower reports and analyzing data for trends.** Helpful metrics include how often the hotline is used, what geographies or business units most frequently use it, what actions the company takes to follow up on claims, and what percentage of claims are substantiated. Several participants recommended having the audit committee review reports at every committee meeting. Some review data even more frequently, with one audit chair noting that weekly reports have improved fraud oversight. Whistleblower reports should be thoroughly analyzed for trends. One participant advised *"specifically looking out for multiple allegations around a similar issue, site, or group of individuals."*

- **Educating employees about issues that the hotline addresses and communicating cultural expectations.** Audit chairs expect management to educate employees on what types of reports and behavior should be reported. For example, one described a situation where the company wanted to focus on a specific data integrity issue. The company let employees know that this type of information was an area of focus and that there was a risk of fraud associated with it. This led to a significant number of tips related to the matter. *"Make sure people understand what whistleblower systems can cover,"* the audit chair said, suggesting the use of informational posters in common areas like hallways and elevators to promote the hotline. As appropriate, policies and communications should be implemented to ensure external stakeholders are aware of fraud hotlines. The 2022 ACFE report found that "more than half of all tips came from employees, while nearly a third of tips came from outside parties, including customers, vendors, and competitors."[7]

> "Make sure people understand what whistleblower systems can cover."
>
> —Audit Chair

- **Establishing benchmarks.** Internal and external benchmarking data—for example, across business units, industries, and countries—is a useful way to compare a company's whistleblower reporting patterns to others. Results that vary significantly could indicate that whistleblower systems are not functioning effectively. One audit chair said, *"We had a relatively small number of reports compared to benchmarking against other companies in our peer group. Our figures were very low ... It's nice to think that is because there were no issues, but we felt it was much more likely due to the fact that people are reluctant to use the system."*

- **Closing the loop with whistleblowers and communicating outcomes.** Reporting back to the whistleblower and appropriately communicating outcomes throughout the company are essential to building trust and creating a positive speak-up culture. *"It makes it clear* *that if a whistle is blown, attention is paid and, when appropriate, corrective actions are taken,"* one audit chair said.

Use technology to help combat fraud

The scale and complexity of fraud risk at large public companies can be daunting for boards. Rapid digital transformation, ever-growing volumes of data, and the increased prevalence of remote work have created new and heightened fraud risks. As a result, companies are increasingly including fraud as part of risk assessments. They also are relying on technology to help combat fraud. One audit chair pointed out that *"fraudsters are using technologies like AI [artificial intelligence], so technology is essential to address it."*

Fortunately, technological developments in machine learning, AI, and data analytics can help overcome some of the challenges of scale and geographic distance. While many companies are still navigating how to effectively deploy technology to combat fraud, these tools are quickly becoming essential, audit chairs said. They discussed important considerations for audit committees:

> ***"The audit committee can be most effective in combatting fraud when it addresses the connections between external audit, internal audit, compliance, risk management, and its own responsibilities. Problems typically arise when those functions work in silos."***
>
> *—Mike Savage, EY Global Forensic & Integrity Services Leadership Team Member*

- **Integration of reporting and data analytics.** Leading audit committees are taking an integrated approach to assessing data as they look for fraud risk. *"Rarely does bad behavior come out of nowhere; there are usually red flags,"* one audit chair said. *"The more we can compile data from various company sources, the more chance we have of picking up potential issues."* This audit chair described how the company created a *"common database to look at internal audit issues, compliance reports, finance issues, culture surveys, whistleblower complaints, and other data points like health inspections."* Data is then analyzed to identify outliers or concerning trends. Mr. Savage observed that *"the audit committee can be most effective in combating fraud when it addresses the connections between external audit, internal audit, compliance, risk management, and its own responsibilities. Problems typically arise when those functions work in silos."*

- **Retention of the human element.** Audit chairs underscored the continued importance of judgment and skepticism, even as the use of technology expands, particularly since technologies like AI can have flawed algorithms and can perpetuate unconscious bias. One participant observed that it is vital to be *"transparent about the assumptions your algorithm is built on,"* and suggested that a third party should check algorithms. *"Anomalies in data should be carefully investigated before conclusions are drawn,"* the participant continued. Mr. Savage agreed, suggesting *"deployment of several algorithms* *coming at it from different angles or other compensating methods to find flaws in the algorithms sooner."* Ms. Weghmann added that audit committees can *"use technology to get indicators, themes, outliers, or interesting commonalities, then dive deeper to do an in-depth analysis from experts within different disciplines."*

- **Understanding external auditors' technology use.** External auditors are increasingly moving toward data-driven audits and using technology for fraud detection. Their experiences can provide useful insights for audit committees. As one audit chair said, *"I haven't historically expected external auditors to be as much help in uncovering fraud, but that has changed because of technology and AI systems."* But Mr. Savage cautioned that even the most technologically advanced audit firms can struggle to access client data. *"Amalgamating the volumes and different types of client data presents challenges for the audit firms,"* he said, but *"once they have it, they can do a lot more with it at effectively no incremental cost."* Participants agreed. *"When you talk to auditors about why they don't use technology more, the answer is that companies aren't ready to deal with it,"* one said. As the use of technology grows, audit committees should speak with their auditors to make sure they understand its capabilities and how it is being deployed.
- **Proactive technology deployment.** Many companies use technology for fraud detection, but it is less commonly used for prevention. This could be a missed opportunity, audit chairs said. One described a good practice of ensuring all new controls are technology based, not manual, which ensures consistency and creates a digital record. Another described using technology to deter employees from improperly downloading data. The company implemented prompts that ask users to confirm their actions: *"It creates a barrier and is one way to use technology as a prevention tool."*
- **Cooperation with management to address obstacles to implementing technology.** Many factors may slow the adoption of antifraud technologies. Members cited high costs of implementation versus the perceived benefit as a potentially significant barrier. Lack of understanding of the role technology can play in fraud prevention and detection can also incline management to believe that existing processes are sufficient. Members also identified lack of talent as a potential barrier: the skills needed *"are scarce and will be in demand,"* one said.

Prepare for frauds associated with ESG data and reporting

With standard setters and regulators implementing ESG reporting requirements, audit chairs are beginning to think about related fraud risks.

ESG fraud is new enough that its scope and range are not entirely clear. An audit chair remarked, *"If a supplier had requirements to meet certain ESG commitments and they misrepresented that, I hope our due diligence would test and find it, but we wouldn't necessarily think of it as fraud."* Another asked, *"Is greenwashing fraud?"* [8]

Participants agreed that ESG fraud has the potential to become a substantial risk. *"We haven't necessarily linked ESG to fraud, but I can imagine how it would become more of an issue as* *the stakes go up,"* one said. ESG matters *"will drive difficult decisions for companies,"* another observed. *"Will companies actually move away from suppliers who can't or won't change? Could it lead to falsification of information? It opens companies up to all sorts of risks."*

Looking ahead, participants underscored the need for audit committees to proactively incorporate ESG into fraud risk assessments. Being aware of *"what could go wrong"* scenarios will be key, Mr. Savage advised. Specifically, audit committees should be attuned to the following:

- **Investor and regulatory pressure.** Heightened attention from regulators and investors may create pressure for companies to appear well positioned to meet targets or comply with future regulations.
- **ESG-linked incentives.** Fraud risk *"is a concern as we link more and more ESG metrics to incentives, particularly remuneration plans,"* a member observed. As companies develop new key performance indicators for ESG-related goals and tie them to executive compensation or other incentives, fraud risk rises.
- **Cultural change.** Culture plays the same crucial role in curbing ESG fraud that it does with other forms of fraud. Employees unfamiliar with the rigors of reporting processes may take on responsibilities for ESG reporting without understanding the difference between *"reporting responsibilities versus trying to meet management's expectations,"* one member said. Audit committees should ensure that teams are appropriately trained and that culture and tone at the top reinforce that the company's integrity is more important than meeting goals.

Increase audit committee and board education on fraud risk

All participants agreed that their audit committees play a major role in overseeing fraud risk. But fraudsters, like cybercriminals, are constantly innovating, finding new points of weakness, and using new methods of attack. Participants felt that boards, and audit committees in particular, might benefit from regularly updated fraud awareness training.

Few audit chairs reported that their boards provide fraud-specific education, but all agreed that focused training could be valuable, especially for newer audit committee members. Real-life examples provide one of the best training opportunities. *"Case studies give you a different perspective to look at what is happening and potentially bring about some changes in your own oversight and supervision procedures,"* an audit chair said. It can be especially helpful for audit committees to learn not only how the fraud occurred, but also how the audit committee handled the situation and the remedial actions taken.

A hands-on learning experience for audit chairs

In response to audit chairs' interest in fraud education and their concerns about emerging ESG fraud risks, Tapestry Networks and EY piloted a fraud simulation training with members of the European Audit Committee Leadership Network (EACLN) in December 2022. The session simulated an audit committee meeting at a fictitious company. Audit chairs played the role of committee members. At the start of the meeting, they were informed of allegations of financial fraud from a short seller. While the company and its details were fictional, the financial reports provided to participants were taken from an actual case of financial fraud.

The simulation enabled members to walk through the process of assessing a fraud allegation, deciding how to respond, informing or involving relevant internal and external stakeholders, and determining an action plan. Afterward, EY leaders provided members with feedback on two fronts: process, including how the audit committee dealt with the allegations; and substance, including which red flags—such as inconsistencies in the draft financial statements, culture, and ESG reports—were identified and where the audit committee could have investigated further.

Fraud Role Play Exercise	Outcomes and Results
• During a simulated audit committee meeting, members learned of financial and sustainability fraud allegations • Clues were drawn from real-life frauds and provided in preparatory materials and during the exercise • Participants planned the audit committee's initial reaction and response, evaluated different sources of information, and developed stakeholder communication plans	• Discussed leading practices to deal with allegations of fraud in line with regulator expectations • Deepened understanding of factors that contribute to a strong corporate governance and compliance culture • Encountered examples of ESG fraud • Gained real-time feedback on how to improve personal and committee-wide responses to fraud allegations

Overall, audit chairs found the session highly useful as a form of dynamic training. One participant noted that *"having different perspectives and cognitive diversity around the audit committee table led to a better investigation."* This became clear as each committee member approached the information in a distinctive way and raised different questions to identify the problem and steps that the audit committee should take. Others emphasized the benefits of receiving feedback from EY. *"We don't get feedback as much as we used to, and it is very useful."* Members believed that such training would be beneficial for audit committees.

For additional detail on lessons learned during the simulation, please see Appendix 3.

Conclusion

Even in large and well-established companies, combating fraud remains a constant challenge. Assessing risk of fraud often comes down to factors that can be hard to measure. New technologies, data sets, and risk environments like cyber and ESG all contribute to the constant evolution of fraud risk for global companies.

Participating audit chairs discussed good practices for audit committees to implement. A foundational step is to ensure that all lines of defense at a company—management, internal audit, external audit, and the audit committee—have clearly defined roles and responsibilities in the fight against fraud and function effectively with the right controls and processes in place. Audit chairs are also increasingly relying on comprehensive cultural assessments, whistleblower systems, technology, and integrated data analytics as vital tools to identify concerning trends and warning signs. Overall, it is essential that audit committees adopt a proactive approach, and many could benefit from regularly updated fraud awareness training.

Appendix 1: Reflection questions for audit committees

Consider the questions below when discussing how your audit committee could strengthen its fraud risk oversight.

Fraud Risk Oversight

- What are your highest-priority fraud risks? How do you monitor how risks may change?
- What are your expectations of management, internal audit, and external audit for detecting and preventing fraud? Do you define clear roles? Are there any gaps?
- How is fraud risk effectively owned, assessed, and communicated across internal functions (e.g., compliance, legal, risk)?
- How effectively does your company collect, respond to, report on, and escalate whistleblower tips? Do employees know what to look for and how to use the hotline?
- How does your audit committee assess if hotlines are working? Do you benchmark your data?

Culture and Cognitive Biases

- How does your audit committee assess culture as part of fraud risk assessments?
- What is management measuring and reporting related to culture? How effective are their tools at identifying indicators of fraud risk?
- What other cultural data would strengthen fraud risk oversight?
- How can audit committees determine if an appropriate tone at the top is in place? How can they check if the message is understood throughout the company?
- How do you use internal and external audit for insight into culture and compliance?

Technology

- How is your company integrating technology into fraud prevention and detection? How comfortable are you with your understanding of how these technologies are being deployed? What concerns do you have?
- What questions does your audit committee ask internal and external audit about the use of technology in the audit? What would you like to understand better?
- What types of data or trend analysis help identify fraud and give early signals of high-risk areas?

Equipping the Audit Committee

- What type of training or education does your audit committee receive related to fraud?
- How confident are you in your audit committee's preparedness to handle a serious fraud allegation from both a process and substance perspective? What type of training would enhance your audit committee's readiness and awareness?
- What concerns do you have around fraud related to ESG and nonfinancial reporting? How might ESG matters raise fraud risk in the coming years?

Appendix 2: Research program and participants

In phase one, completed in 2020 and 2021, Tapestry convened a small group of audit chairs from the European Audit Committee Leadership Network (EACLN), which includes some of Europe's largest global companies, to discuss fraud-related issues. The project resulted in a submission to the International Auditing and Assurance Standards Board during their consultation period for the drafting of new auditing standards for fraud.[9]

In phase two, held in 2022, Tapestry again assembled a group of EACLN members to further outline responsibilities, expectations, and good practices for audit committees as they work to combat fraud.

Objectives and process

For phase two, Tapestry offered four workshops focused on identifying tools and methods that audit committees can employ to improve their oversight of fraud risk, such as clarifying expectations for management, internal audit, external audit, and audit committees themselves related to fraud prevention and detection.

In addition, Tapestry held two sessions on corporate fraud during meetings of the European Audit Committee Leadership Network to gain input from a larger group of leading European audit chairs. The first session explored lessons learned from Wirecard, the now defunct German fintech company, as a case study on corporate fraud. The second piloted a simulation in which EACLN members assumed the roles of audit committee members for a fictitious company and worked to uncover an alleged fraud. Prior to each session, participating audit chairs shared their perspectives on fraud-related issues during one-on-one calls with Tapestry.

The workshops and EACLN sessions covered the following topics:

- **The governance ecosystem**—expectations of management, internal audit, and external audit
- **The role of the audit committee**
- **The future of fighting fraud**
- *Corporate fraud—Wirecard as a case study* [10]
- **Audit committee simulation and role-play**

All discussions were held under a modified form of the Chatham House Rule whereby comments may be quoted, but without attribution to an individual or company. Audit chairs spoke on their own behalf rather than as representatives of their companies or boards. EY provided financial support for the research and writing of this report and had opportunities to comment on the research design and the final product but did not exercise any editorial control. Tapestry bears full editorial responsibility.

Participants

Nine current and former audit chairs participated in the research workshops for the fraud project between April and November 2022:

- Alison Carnwath, BASF and Zurich Insurance
- Liz Doherty, Novartis and Philips
- Eric Elzvik, Ericsson
- Liz Hewitt, National Grid and Glencore
- Arne Karlsson, Mærsk
- Dagmar Kollmann, Deutsche Telekom
- Guylaine Saucier, Wendel
- Alan Stewart, Diageo
- Maria van der Hoeven, TotalEnergies

Additional perspectives were gained from the following audit chairs, who participated in the EACLN sessions focused on corporate fraud held in September and December 2022:

- Jeremy Anderson, UBS
- Werner Brandt, Siemens
- Julie Brown, Alumna
- Ana de Pro Gonzalo, STMicroelectronics
- Carolyn Dittmeier, Assicurazioni Generali
- Byron Grote, Tesco and Akzo Nobel
- Marion Helmes, Heineken
- Pilar López, Inditex
- Benoît Maes, Bouygues
- John Maltby, Nordea
- David Meline, ABB
- Marie-José Nadeau, ENGIE
- Karyn Ovelmen, ArcelorMittal
- Nathalie Rachou, Veolia
- Erhard Schipporeit, RWE

Appendix 3: A simulated audit committee meeting—feedback and lessons learned

A key learning component for audit chair participants in the 2 December simulated audit committee meeting addressing fraud was learning which aspects of their responses were successful and when different approaches would have led to better outcomes. The facilitators and creators of the session—Tapestry Networks and EY—provided feedback and observations in two areas:

Process	Substance
The process aspect of audit chair participants' response to the simulation was strong. Members embraced the role-play, were actively engaged, grasped the importance of the new information, correctly adapted the meeting to the new circumstances, and proceeded with their initial assessment of the allegations. Feedback was provided in key areas: • Initial response • Assessment of available information • Defining the audit committee's role • Interviewing and/or briefing internal stakeholders • Involving outside parties, including counsel, external auditors, etc. • External stakeholder communications	Members received coaching on the substance of the case, including on recognizing key clues in the preread materials and video presentations, as well as clues revealed during the meeting. Those included: • Financial reporting red-flags • The short-seller report • HR survey and cultural indicators • The draft sustainability report

Endnotes

[1] This report uses of a modified version of the Chatham House Rule whereby names of participants and their company affiliations are a matter of public record, but comments are not attributed to individuals or corporations. Italicized quotations reflect comments made in connection with our research.

[2] European Audit Committee Leadership Network, *Corporate fraud—Wirecard as a case study*, ViewPoints (Waltham, MA: Tapestry Networks, 2022), 3.

[3] *International Standard on Auditing (ISA) 240: The Auditor's Responsibility to Consider Fraud in an Audit of Financial Statements* (New York: International Auditing and Assurance Standards Board, effective December 15, 2004), 275.

[4] European Audit Committee Leadership Network, *Corporate fraud—Wirecard as a case study*, 2.

[5] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations* (Austin, TX: Association of Certified Fraud Examiners, Inc., 2022), 2, 4.

[6] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations,* 22.

[7] Association of Certified Fraud Examiners, *Occupational Fraud 2022: A Report to the Nations*, 21.

[8] "Greenwashing" is a term used to describe attempts to make products or services appear more environmentally friendly than they truly are.

[9] Tapestry Networks, *Fighting fraud: Conversations with leading European audit committee chairs* (Waltham, MA: Tapestry Networks, 2021).

[10] European Audit Committee Leadership Network, *Corporate fraud—Wirecard as a case study*.