Deloitte.

A proactive defense: A survey on the fraud risk assessment experience

Early revenue recognition to meet earnings targets. Kickbacks to vendors and third parties. Theft of inventory for personal gain. Invoices submitted and paid for services never delivered. Fraud continues to be a valid concern in the business world—and the amount lost to fraud continues to challenge organizations' operational risk profiles.[1]

A fraud risk assessment (FRA) is a scheme and scenario-based risk assessment designed to identify, assess, prioritize, and respond to potential fraud risks facing an organization. The aim is to think about how someone might commit a fraud against the organization and whether the organization has appropriate controls to mitigate the chances of that fraud happening.

Formal FRAs could cut median fraud loss by 45%, but companies don't always perform them.[2] That leaves many companies unaware of what frauds they could fall victim to or how to protect themselves against these frauds.

To get a better idea of companies' experiences with FRAs, we carried out a survey at organizations across a variety of industries, and 73 executives responded. We focused our questions on how respondents use FRAs in their organization, the components of these assessments, where within organizations fraud risk management occurs, and where within companies are facing challenges in designing and implementing their FRAs as part of their broader fraud risk management program.

Here's what we discovered—and what our findings could mean in the context of an organization's larger fraud risk management considerations.

A pillar of fraud risk management

An FRA is one of five elements that make up a broader fraud risk management program. The other four elements are:

- **Governance and the control environment**, including the policies and procedures that are in place and those who are responsible for them.
- **Preventive and detective control activities** such as appropriate review and approvals, segregation of duties, delegation of authority, and restricted access.
- **Information, communication, and awareness** such as a code of conduct or ethics training, employee acknowledgment of policies, and proactive ethics hotlines and ethical communications.
- **Investigation, response, and monitoring** related to suspected fraud—including intake, triage, investigation, remediation, and ongoing monitoring.

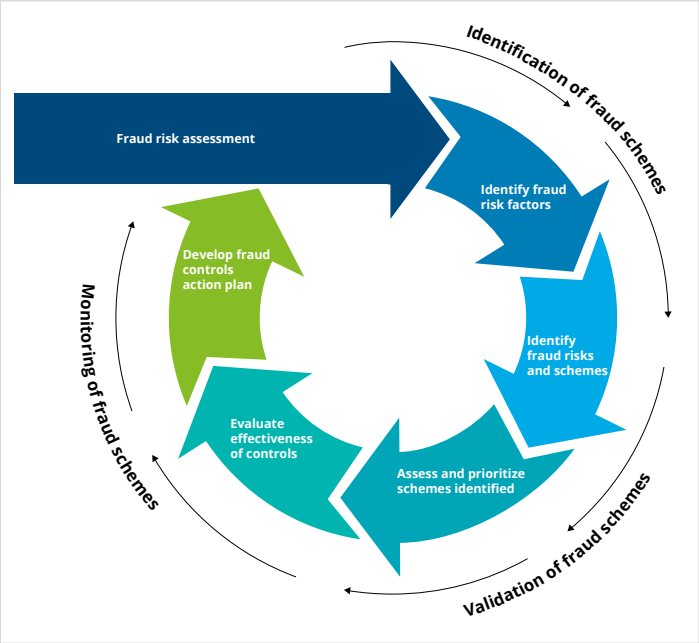
80% of the respondents to our survey said that fraud risk management is a component of their broader enterprise risk management activity.

Nearly three-quarters of the respondents indicated their organization has a fraud risk framework in place. 92% of public company respondents have an established fraud risk framework, while only 56% of private company respondents answered affirmatively. 93% of respondents working at companies with $1 billion or more in annual revenue reported the existence of fraud risk frameworks, whereas 45% of respondents from companies with revenues under $1 billion reported the same.

From an industry perspective, most respondents said a fraud risk management framework exists in their organization. Financial services and energy and resources—both highly regulated industries—lead the pack (figure 1).

Figure 1. Existence of fraud risk management framework by industry (top four industries)

Figure 2. The FRA process



FRA foundations

Suppose a company's initial public offering places new pressures to meet earnings expectations and satisfy many new stakeholders. That's a *fraud risk factor.*

Executives could succumb to this pressure when performance doesn't match projections or expected results, and manipulate earnings to achieve those targets. That's a fraud risk.

A *fraud scheme* describes how a fraud risk could become reality. In our example scenario, management might manipulate earnings by recording a shortened contract term to accelerate revenue recognition. Or it might invoice customers prior to shipment and allow longer payment terms. Another possibility is to delay recognition of current-period expenses. A variety of other schemes may exist as well.

The FRA portion of a comprehensive fraud risk management program should be an ongoing process (figure 2). For example, companies can consider revisiting the process throughout the year as significant events occur, in addition to refreshing it periodically.

The FRA process typically begins with the identification of fraud risk factors (and not just from a financial reporting perspective). Fraud risk factors can span operations, geographies, and other dimensions of a business. The scenarios can be just as diverse: think merger or acquisition, a change in management or business structure, or new organizational initiatives, products, or services.

After identifying fraud risk factors, the next step is to determine what the actual fraud risks are and what shape the associated fraud schemes might take. The list will likely be long, making it necessary to prioritize. Consider the likelihood, impact or significance, potential for management override, and absence of internal controls to identify the inherent risk for each fraud scheme. Once prioritized, it's important to identify and map or link existing internal controls to the prioritized fraud schemes, considering both preventive and detective controls.

While Sarbanes-Oxley internal controls may cover many of the fraud schemes, operational controls should be identified as well. Finally, conduct or leverage the results of control testing to determine if they're operating effectively. Where they aren't, or where adequate controls are missing, remediate.

Internal fraud—the areas of most concern

Our survey focused on internal fraud or fraud committed by employees, managers, and executives inside the company. Against that backdrop, breaches of internal ethical or compliance policy are the most widespread concern, cited by 76% of respondents, followed closely by violations of laws and regulations. These two cover a wide variety of conduct that goes beyond direct asset misappropriation. By comparison, 51% cited theft or embezzlement as the risks that worry them the most—still a sizable portion of respondents, but tied for third as an area of concern. Respondents were least concerned about complicated or creative accounting although a similar category, financial reporting manipulation, was tied for third-most frequent area of concern (figure 3).

In addition, Paul Munter, then acting and now current chief accountant at the US Securities and Exchange Commission (SEC), pointed out in an October 2022 statement that even small misstatements due to fraud can be material.[3] Materiality goes beyond numeric values. Recent SEC statements indicate that qualitative materiality may be equally as important to regulators.[4] This could include, for example, cases where the dollar value of the fraud might not have been material to the financial statements or a key performance indicator, but the perpetrators' actions were intentionally deceptive or intentional violations of securities laws. The intentionality makes the fraud qualitatively material, meaning the information would matter to investors or others who rely on the company's financial statements to make decisions.

Qualitative materiality may have an even broader application from a regulatory purview. We continue to see "books and records" cases in which ongoing material weaknesses in internal controls are cited as securities violations, even if no financial loss occurred.[5] The SEC is also bringing cases for misleading financial statement users by including performance measures not in line with generally accepted accounting principles (GAAP), which do not directly touch the financial statements but can influence investors' decisions.

What can companies do? Consider the regulatory environment in which your business operates and the disclosures your company makes while designing your FRA.

How current approaches are working

We asked respondents about the perceived effectiveness of both their organization's fraud risk management framework and the fraud risk assessment within that framework.

Figure 4. Top barriers to fraud risk management framework effectiveness

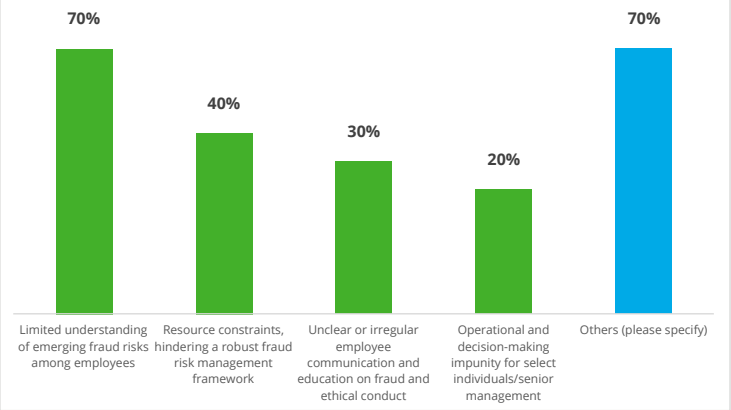
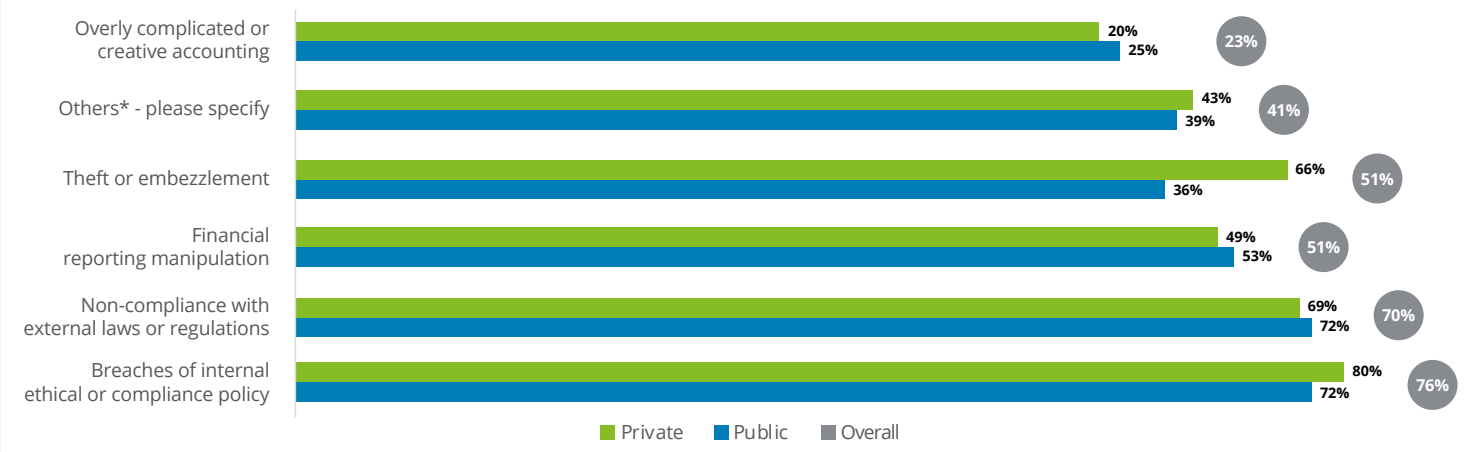


Figure 3. Areas of internal fraud concern

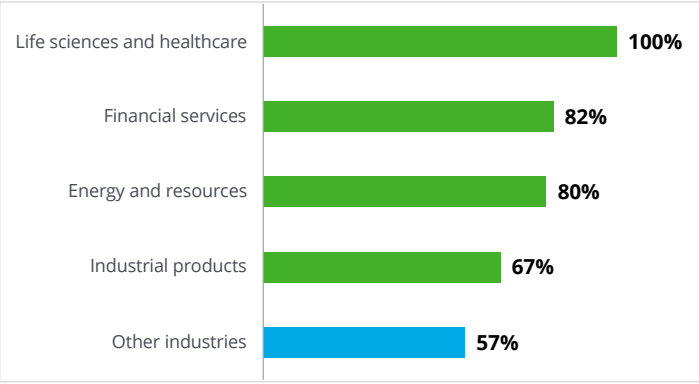


In total, about 81% of our respondents said their organization's current fraud risk management framework is effective or very effective. The 19% who said it isn't credit a variety of several reasons, the most common being a limited understanding of emerging fraud risks among employees (figure 4).

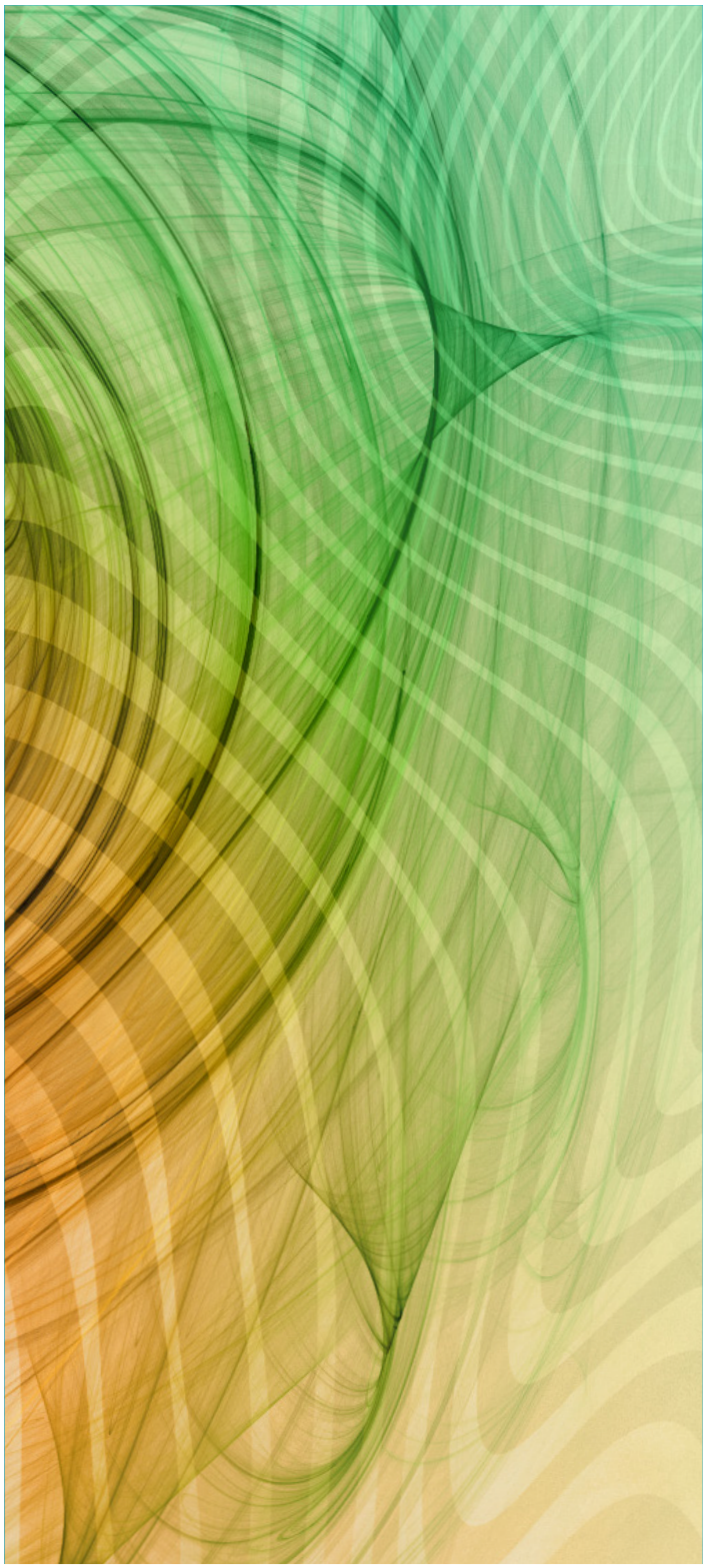
A significant share of this group also cited a reason that wasn't a response option: denial culture, or the belief that fraud can't happen at their organization. This is the number-one feedback in the "Others" category.

By the same token, 73% of companies considered their FRAs within the fraud risk management framework to be effective or very effective at reducing internal fraud. An industry breakdown reveals more detailed insights. All the respondents who work in life sciences and health care, consumer services, and aerospace and defense said that their FRAs were effective, followed by 87% of respondents who work in financial institutions. On the flip side, respondents in the technology, media, and telecom and retail, wholesale, and distribution industries said their fraud risk assessments were not effective (figure 5).

Figure 5. Overall perceived effectiveness of fraud risk assessment by industry



Life sciences and health care	100%
Consumer services	100%
Aerospace and defense	100%
Financial services	87%
Consumer products	86%
Energy and resources	79%
Industrial products	76%
Others	60%
Professional services	50%



Of the 28% of respondents who did not consider their FRAs to be effective we asked what was preventing their effectiveness. Most (64%) said the biggest reason their FRA is not effective is because it's treated as a tick-the-box exercise (figure 6).

Figure 6. Top factors inhibiting existing fraud risk assessments

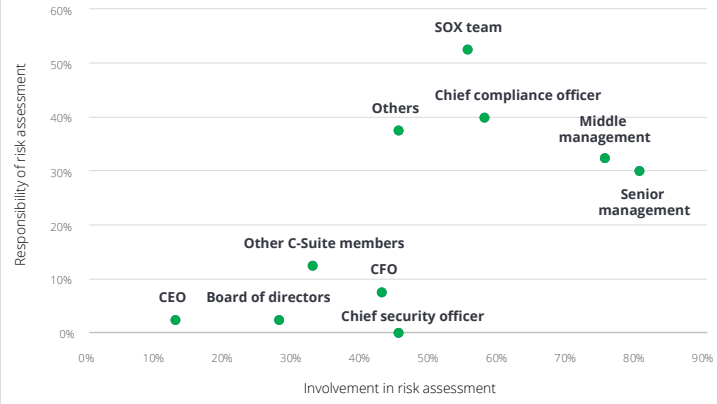
1. Assessment treated as a "tick-the-box" exercise	**64%**
2. Assessment is not performed regularly enough	**55%**
3. Assessment treated as an afterthought during regular work on internal controls	**45%**
4. Assessment is not refreshed throughout the year	**36%**
5. Lack of follow-up action based on results of the assessment	**36%**

Even if companies are dedicated to developing and maintaining a thoughtful FRA, companies may not have the resources to work through the scenarios and schemes underlying the assessment. Others may believe existing controls provide adequate coverage. Denial culture again is another possible driver, where it is difficult for a company to believe that fraud can occur in their organization.

The second-most common factor (55%) inhibiting existing FRAs in our survey respondents was that the assessment isn't performed regularly enough. This reflects the need to refresh assessments periodically so they can stay effective in a fast-changing risk environment.

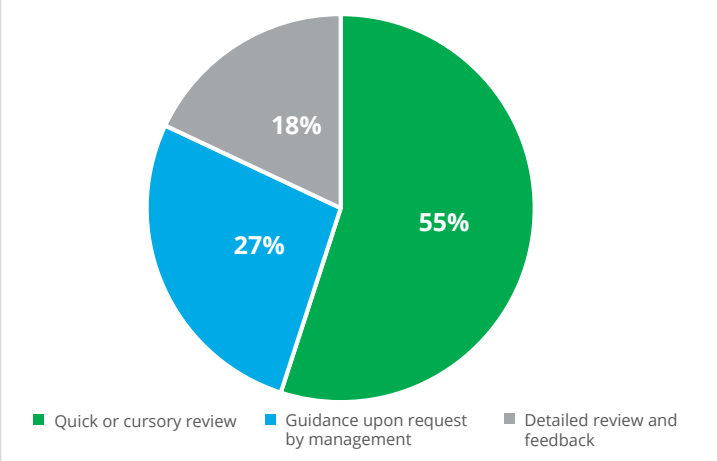
An effective FRA has someone accountable for its creation and success. At the organization for most of the respondents to our survey, responsibility for FRAs primarily fell on the Sarbanes-Oxley team, chief compliance officer, and/or middle to senior management (figure 7).

Figure 7. Parties responsible for the organization's FRA

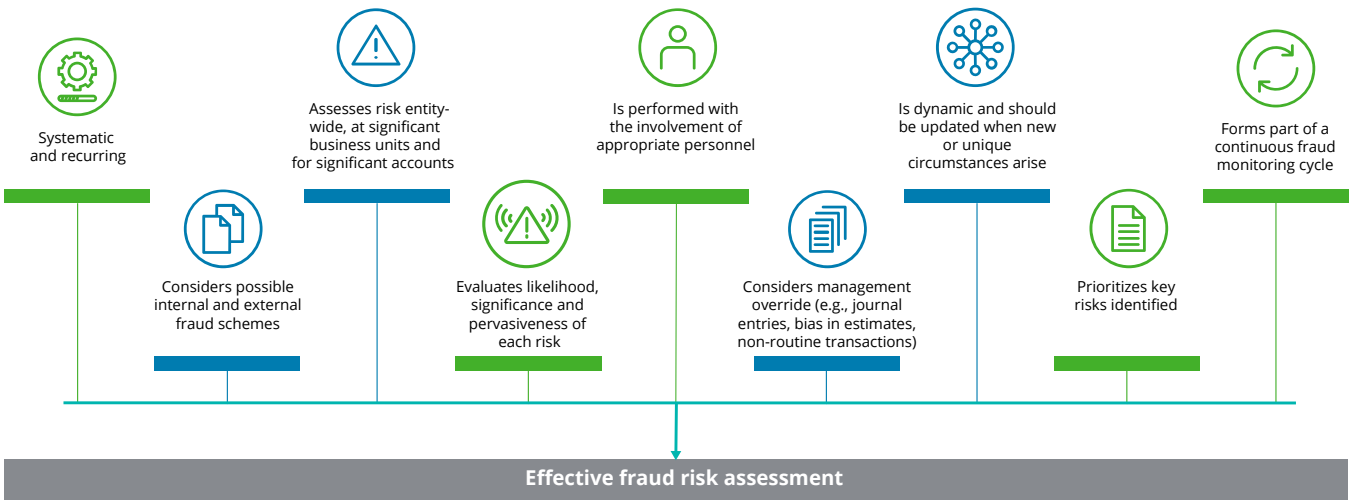


However, only 18% said their board is involved to the extent that it provides a detailed review and feedback (figure 8).

Figure 8. Level of involvement of board of directors in fraud risk assessment



The making of an effective FRA



Taking FRAs to the next level

An FRA is a strong mitigating factor to internal misconduct. Although most of the respondents in our survey reported having an effective fraud risk framework in place, a non-trivial share said they don't. The findings are similar for FRAs.

Where can companies take it from here? Consider the following activities:

- Conduct robust FRAs as part of the overall enterprisewide risk management processes (rather than just going through the motions).
- Combat denial culture by educating employees and stakeholders to increase their understanding of fraud risks and the actions the company has in place to prevent, detect, and deter fraud from occurring.
- Involve appropriate and adequate personnel in the FRA process.
- Consider historical fraud, industry fraud, and recent fraud trends as elements of an enterprisewide FRA.
- Use data analytics to proactively identify potential anomalies that could lead to potential fraud risks and to monitor known fraud risks.
- Once fraud risks are determined, identify different types of fraud schemes and scenarios associated with the risks.
- Deliver on the FRA through fraud controls and action plans.
- Refresh the assessments periodically, including in response to both internal and external factors.
- Communicate the results to management and those charged with governance.

If you have any questions about the analysis arising from the responses received in our survey, or would like to know more about FRA design and implementation, please contact us.

About the survey

73 professionals participated in the Deloitte FRA survey, most of them located in the United States. The survey asked respondents about their experiences with fraud at their organizations and the challenges they face in implementing their FRA.

Figure 9. Survey respondents by role

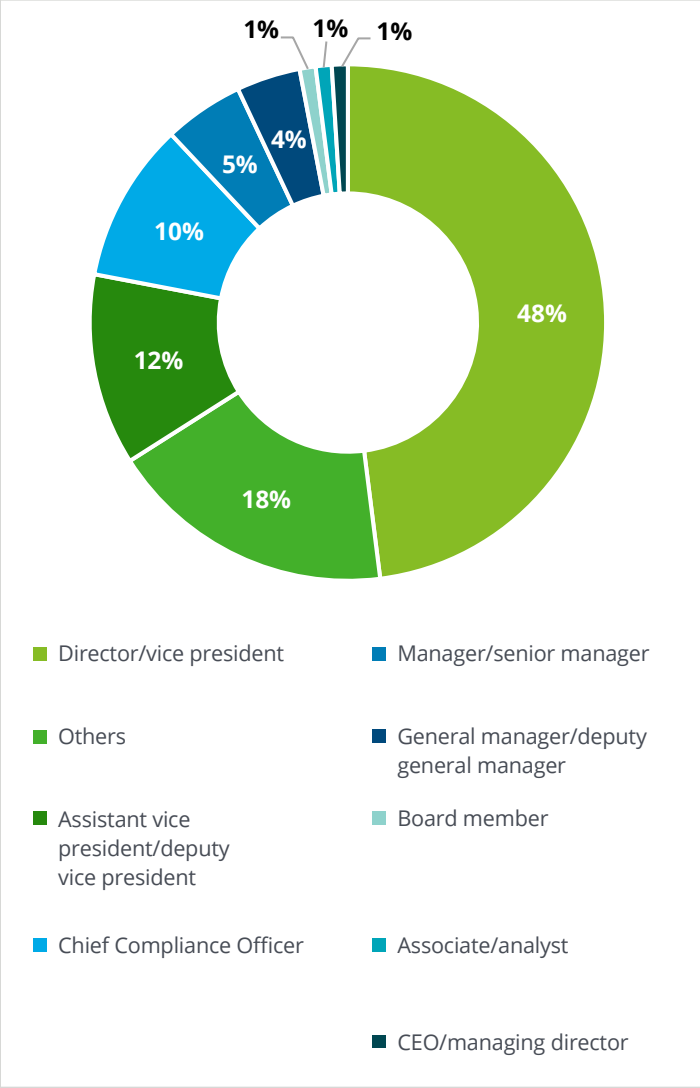


Figure 10. Survey respondents by company ownership

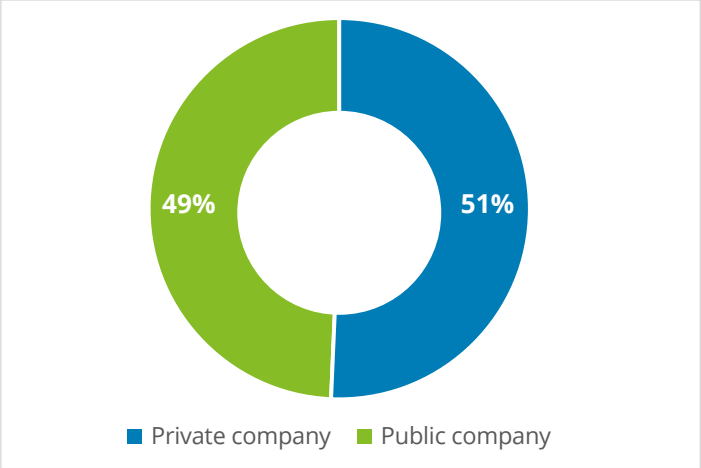
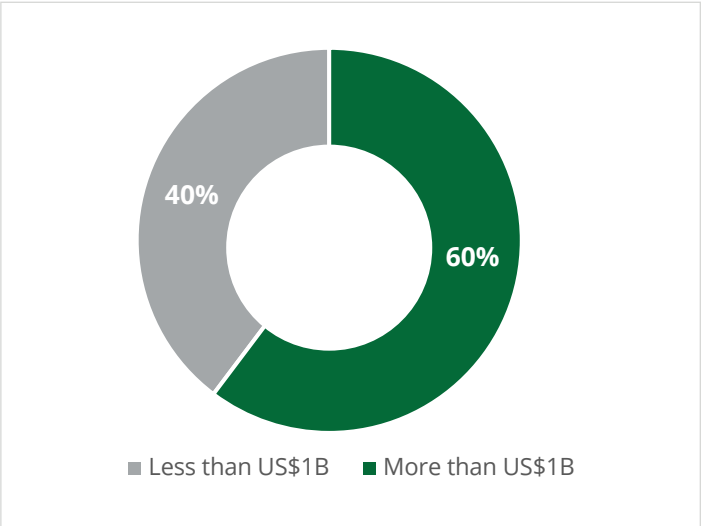


Figure 11. Survey respondents by company revenue



Contacts

Mike Brodsky
Managing Director
Deloitte & Touche LLP
mbrodsky@deloitte.com

Holly Tucker
Partner
Deloitte Financial Advisory Services LLP
htucker@deloitte.com

Sofia Hussain
Senior Manager
Deloitte & Touche LLP
sofhussain@deloitte.com

Endnotes

1. Leslie Fair, "FTC crunches the 2022 numbers. See where scammers continue to crunch consumers," US Federal Trade Commission (FTC), February 23, 2023.
2. *Occupational Fraud 2022.* - https://acfepublic.s3.us-west-2.amazonaws.com/2022+Report+to+the+Nations.pdf.
3. Paul Munter, "The auditor's responsibility for fraud detection," US Securities and Exchange Commission (SEC), October 11, 2022.
4. Paul Munter, "Assessing materiality: Focusing on the reasonable investor when evaluating errors," SEC, March 9, 2022.
5. For example, "SEC charges 16 Wall Street firms with widespread recordkeeping failures," press release, SEC, September 27, 2022.

Deloitte.