Bank Director
Strong Board. Strong Bank.

2026 Risk Survey

SPONSORED BY:

bakertilly

March 2026
Research

TABLE OF CONTENTS

About Bank Director

Bank Director reaches the leaders of the institutions that comprise America's banking industry. Since 1991, Bank Director has provided board-level research, peer insights and in-depth executive and board services. Built for banks, Bank Director extends into and beyond the boardroom by providing timely and relevant information through *Bank Director* magazine, board training services and the financial industry's premier event, Acquire or Be Acquired. For more information about Bank Director, visit **BankDirector.com**.

Bank Director

About Baker Tilly

Baker Tilly is a leading advisory, tax and assurance firm, providing clients with a genuine coast-to-coast and global advantage in major regions of the U.S. and in many of the world's leading financial centers – New York, London, San Francisco, Seattle, Los Angeles, Chicago and Boston. Baker Tilly Advisory Group, LP and Baker Tilly US, LLP (Baker Tilly) provide professional services through an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable laws, regulations and professional standards. Baker Tilly US, LLP is a licensed independent CPA firm that provides attest services to its clients. Baker Tilly Advisory Group, LP and its subsidiary entities provide tax and business advisory services to their clients. Baker Tilly Advisory Group, LP and its subsidiary entities are not licensed CPA firms. For more information about Baker Tilly, visit **bakertilly.com**.

bakertilly

EXECUTIVE SUMMARY

Laura Alix is the director of research for Bank Director, an information resource for directors and officers of financial companies. You can connect with her on LinkedIn.

Adoption of artificial intelligence tools by banks ramped up in 2025, with AI-enabled technologies assisting banks with myriad important functions, from loan processing to customer service to compliance. But AI also introduces new threats.

Bank Director's 2026 Risk Survey, sponsored by Baker Tilly, finds 79% of CEOs, board members, chief risk officers and senior executives concerned about fraud. And when it comes to AI, these banks' leaders are most concerned about fraud and scams targeting their customers (84%) and their employees and organization (77%). The competitive threat from other financial institutions and nonbanks (38%) ranks a distant third concern.

Twenty percent believe their bank or its customers had been impacted by fraud involving AI or deepfake media over the prior 18 months.

Survey respondents broadly indicate at least baseline levels of understanding of many AI-related topics, including machine learning, use cases for AI and data governance. However, a third say they do not understand agentic AI, a newer form of the AI technology focused on autonomous decision making, at all.

Bank leaders don't need to have an extensive understanding of agentic AI or other forms of artificial intelligence, but a basic understanding may be beneficial from a governance standpoint. For example, management ought to at least be able to explain to employees why they shouldn't use widely available AI tools that haven't been vetted by the organization — and could compromise customer and proprietary data — for bank business.

"Banks need a baseline level of understanding so everyone knows what's in play," says Mark Wuchte, Baker Tilly's financial services risk advisory leader. "Without that foundation, you risk people inadvertently using tools outside of the bank's oversight. Governance needs to be part of the conversation from the very beginning."

Changes in the broader competitive landscape due to AI and a rise in fintech firms seeking bank charters is also likely feeding increased concern around strategic risk, Wuchte says. Forty-two percent of survey respondents rank strategic risk as a top area of concern for 2026, up from 30% who said as much a year ago. Separately, 53% of respondents believe their bank could take more strategic risk.

Smaller banks may have once had the luxury of being able to take their time with new strategic directions, but shifting customer expectations are forcing their hand. "They need to get more agile and make decisions more quickly," Wuchte says. "Customer tastes and expectations are changing, so they have to do that in order to stay relevant."

KEY FINDINGS

Regulatory Risk Recedes

With the second Trump administration taking a friendlier regulatory posture toward the industry, just 28% of respondents cite regulatory risk as a top concern this year, down from 55% last year. Forty-four percent say their bank saw heightened attention to liquidity planning or strategy during their most recent regulatory exam, while the percentage who report heightened attention to cybersecurity (37%) increased compared to 2025 (30%).

Learning on the Job

More than a third (35%) of respondents feel the examiner on their bank's last regulatory exam was inexperienced compared with previous exams; and 38% believe their primary regulator was understaffed or otherwise underresourced.

Cybersecurity Oversight

Seventy-nine percent of board chairs and independent directors say the board reviews and approves the bank's cybersecurity strategy, which is set by management. Despite few cybersecurity experts in bank boardrooms, less than half (47%) of directors say the board invited outside experts to speak to cybersecurity trends over the past 12 months.

Identifying Cybersecurity Gaps

A majority (89%) of CEOs and tech executives say their bank has conducted a tabletop exercise of its cybersecurity incident response plan over the prior 12 months. Respondents cite overreliance on one individual or function (36%) and internal communications (35%) as the most common gaps found via that exercise.

Credit Risk Concerns

The percentage of respondents who indicate credit as a top risk increased to 60% from 51% a year ago. Commercial real estate is a particular point of emphasis, with respondents sharing concerns about credit quality (27%) and loan portfolio concentrations (38%) in that loan category.

Risk Responsibility

Fifty-four percent of respondents indicate their bank employs a chief risk officer. Among those respondents, 81% say the CRO reports directly to the CEO, and almost two-thirds say the CRO interacts with directors at every board meeting.

STRATEGIC RISK

1. With respect to your bank, which five risk categories are you most concerned about for 2026?

Respondents were asked to select no more than five options.

92% Cybersecurity

79% Fraud

60% Credit

42% Strategic

42% Interest rate risk

33% Operational

31% Compliance

30% Liquidity

28% Regulatory

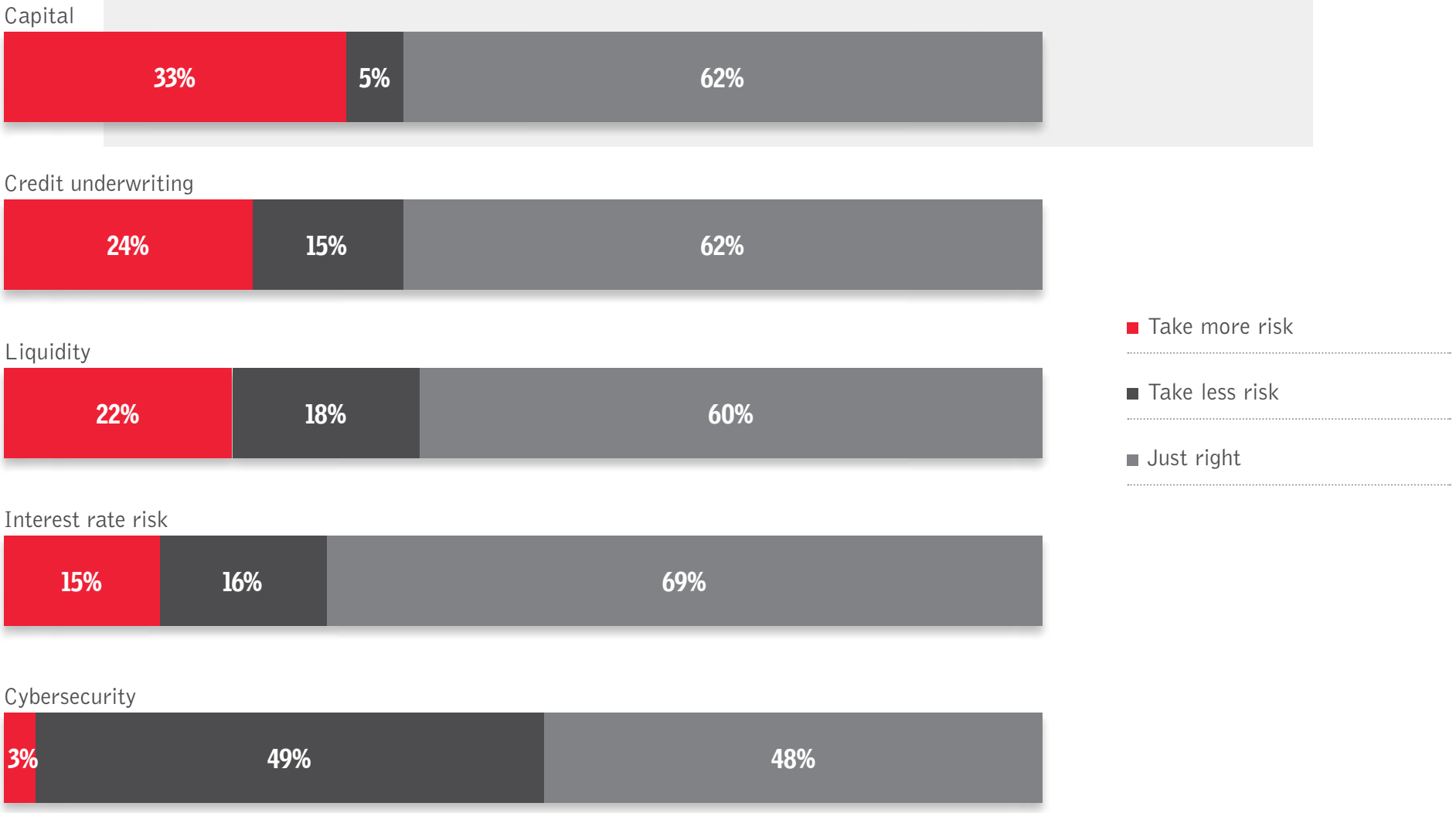
8% Consumer

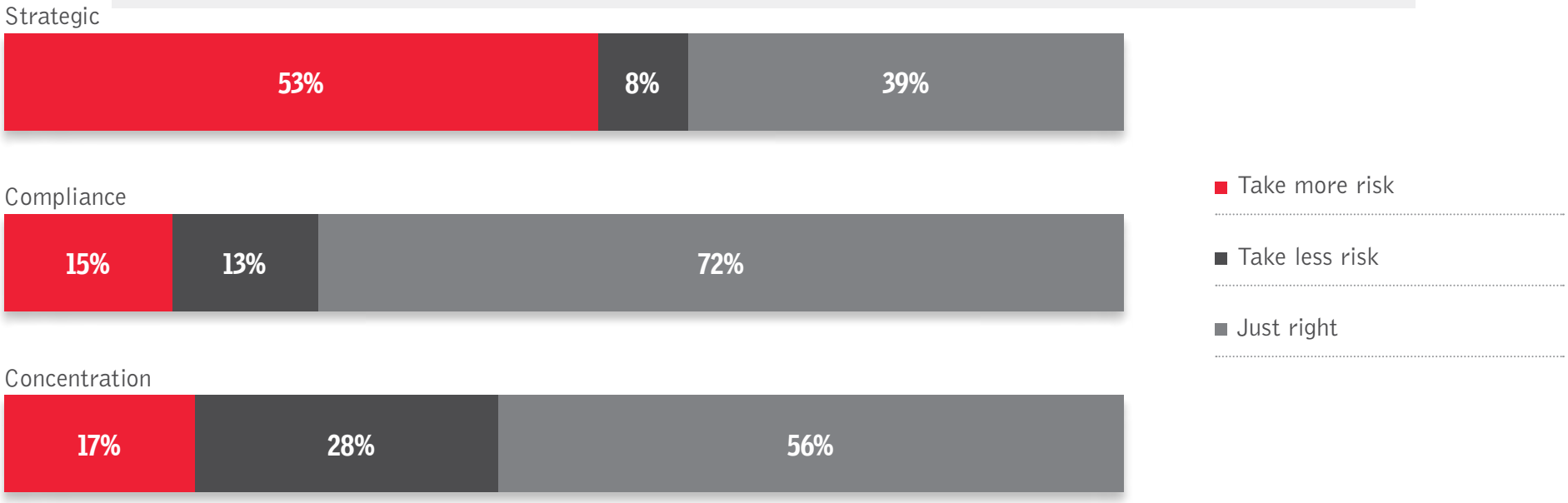
5% Reputational

3% Environmental/climate risk

<1% Legal

2. In what specific areas do you feel your bank could be more aggressive and take more risk, or be more conservative and take less risk?

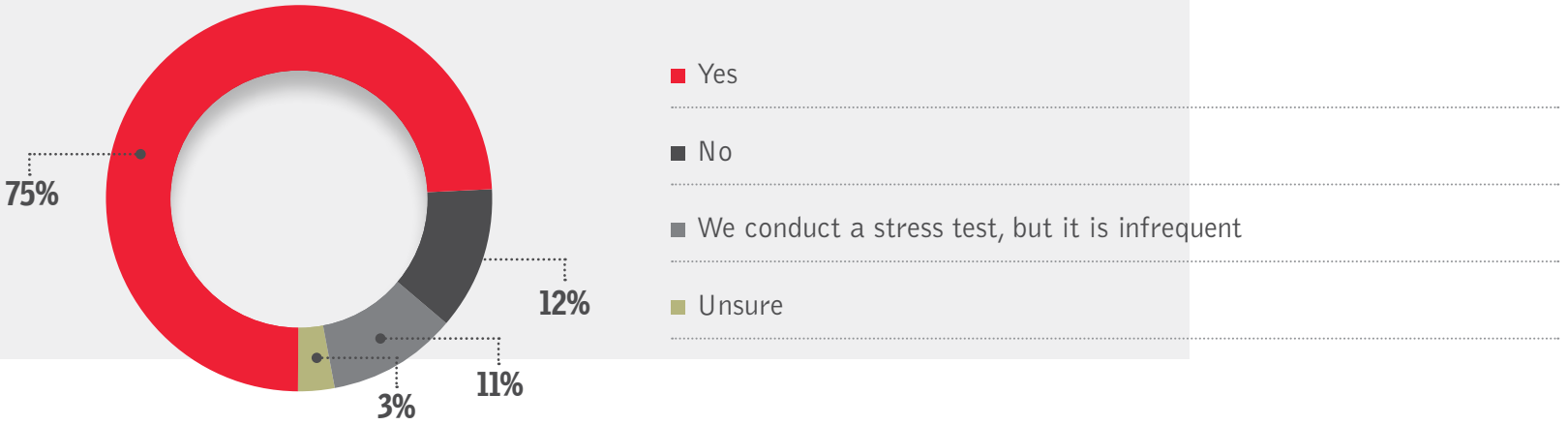




STRESS TESTING & CREDIT RISK

3. Does your bank conduct an annual stress test?

Question not asked of chief information security officers, chief information officers or chief technology officers. Numbers do not add up to 100% due to rounding.

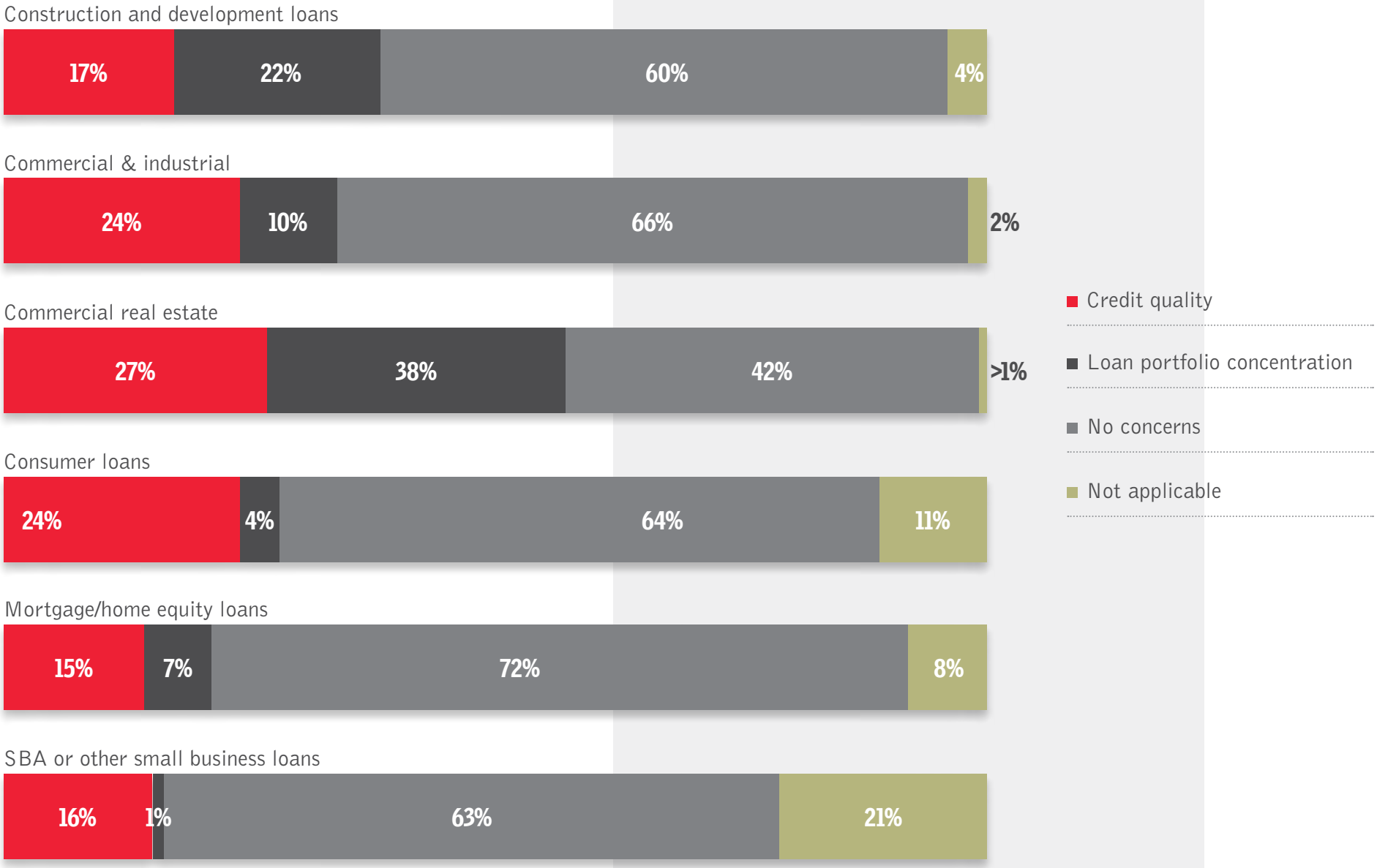


4. How has your bank used the results of its most recent stress test over the past year?

Respondents were asked to select all that apply. Question only asked of respondents who indicated their bank conducts an annual stress test.

38%	We're proactively managing certain commercial real estate credits
36%	We've adjusted our liquidity plan and/or policy
35%	We've adjusted our asset/liability management strategy
35%	We're taking a careful look at loans set to renew in the next six to 12 months
35%	We've adjusted our capital plan and/or policy
25%	We've rebalanced our securities portfolio
19%	We're planning for elevated credit losses in certain categories
15%	We're proactively managing certain agricultural credits

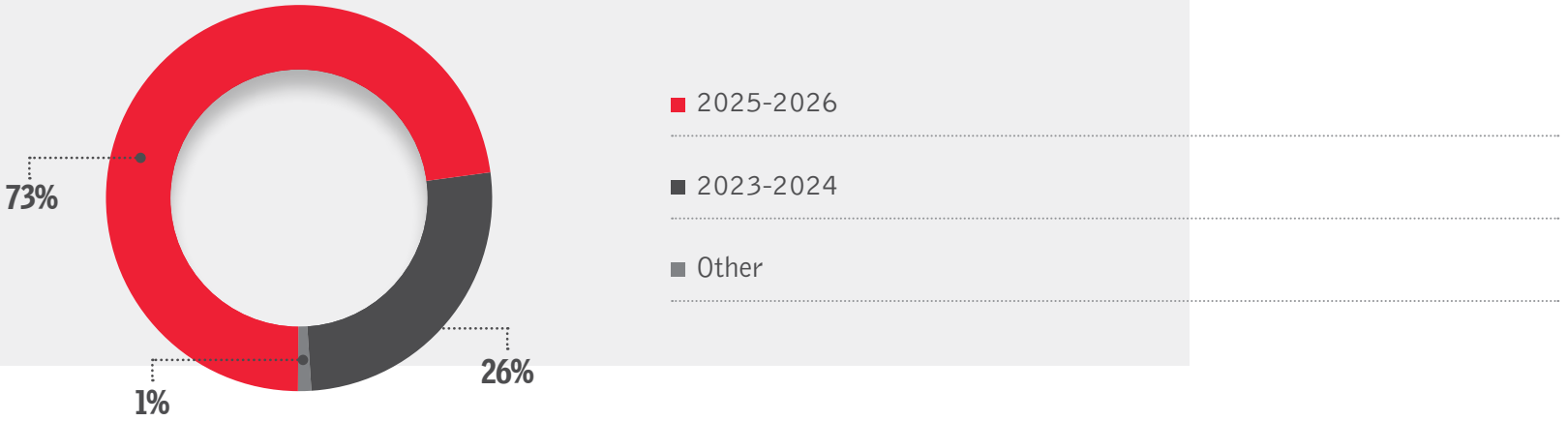
5. Are you concerned about loan portfolio concentrations or credit quality in any of the following areas of your bank's business?



THE REGULATORY ENVIRONMENT

6. When was your bank's last regulatory exam?

Question only asked of chief executive officers, chief risk officers, chief compliance officers, chief financial officers, board chairs and independent directors.



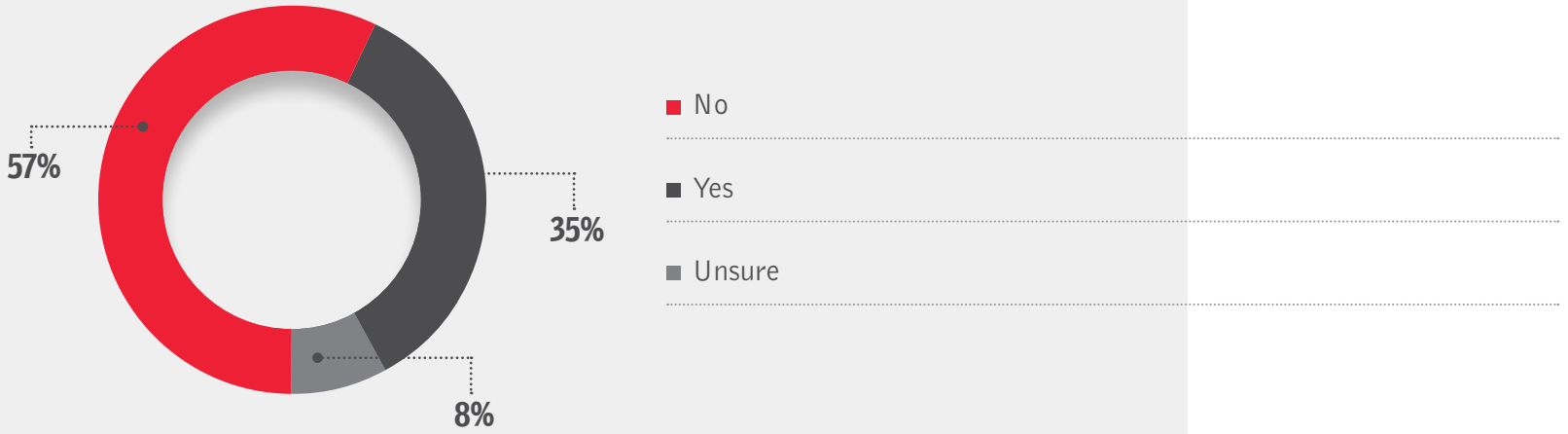
7. In what areas did your bank see heightened attention from its regulators on its last exam?

Question only asked of respondents who indicated their bank's last regulatory exam was in 2023-2024 or 2025-2026. Respondents were asked to select all that apply.

	Total
Liquidity planning/strategy	44%
Cybersecurity	37%
Asset quality	25%
Vendor oversight of third and/or fourth parties	24%
Capital planning/strategy	20%
Bank Secrecy Act/anti-money laundering regulations	18%
Asset/liability management	18%
Regulators did not indicate heightened attention in any specific area	17%
Interest rate sensitivity	16%
Earnings	13%
Management	12%
Community Reinvestment Act compliance	12%
Market risk sensitivity	10%
Overdraft or other consumer fees	6%
Other	5%

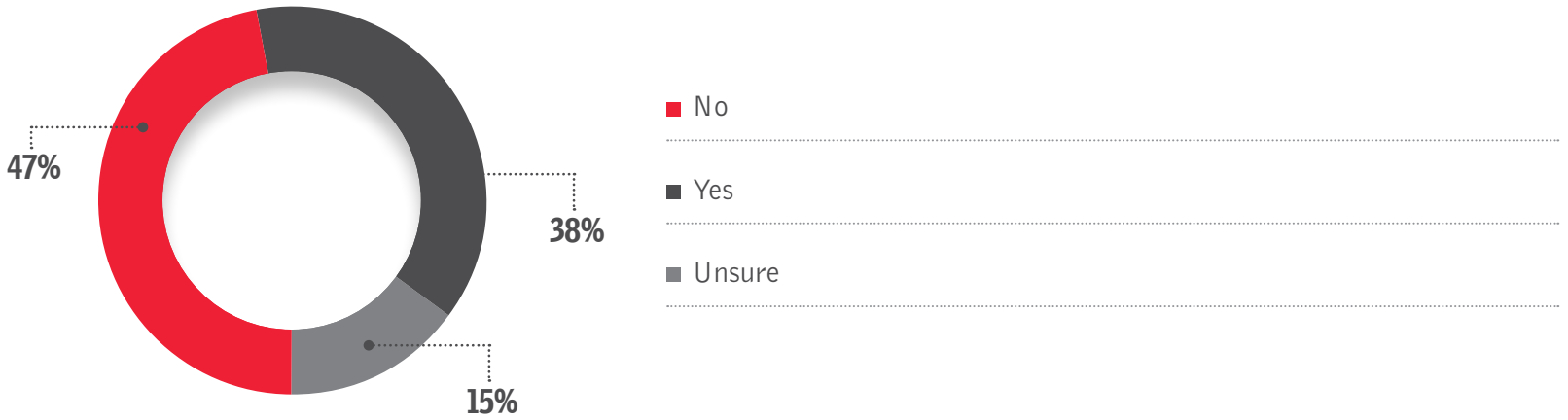
8. Thinking about your most recent regulatory examination, did you feel that your bank's examiner was inexperienced compared to previous exams?

Question only asked of respondents who indicated their bank's last regulatory exam was in 2023-2024 or 2025-2026.



9. Do you believe your primary regulator has been understaffed or otherwise under resourced in 2025?

Question only asked of respondents who indicated their bank's last regulatory exam was in 2023-2024 or 2025-2026.



10. Over the past 18 months, has your bank made any of the following changes to its BSA/AML compliance program?

Respondents were asked to select all that apply. Question only asked of CEOs, CROs, CFOs, chief compliance officers, board chairs and independent directors.

51%	Invested in technology to boost the BSA/AML function
47%	Improved training for frontline employees
32%	Added BSA/AML compliance staff
31%	Improved internal controls
30%	Enhanced BSA/AML reporting to the board
27%	Enhanced customer due diligence
23%	Increased independent review and testing
17%	Our bank hasn't made any of these changes
7%	Implemented direct reporting to the board from the BSA/AML function
2%	Other

FRAUD & CYBERSECURITY

11. Have your bank or its customers been directly impacted by any of the following types of fraud over the past 18 months?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs. Respondents were asked to select all that apply.

99% 

Check fraud

84% 

Financial exploitation of elderly or vulnerable customers

73% 

Digital payments fraud

68% 

ACH/wire fraud

59% 

Identity theft

39% 

Account takeover fraud

20% 

Fraud involving artificial intelligence or deepfake media

16% 

Synthetic identity fraud

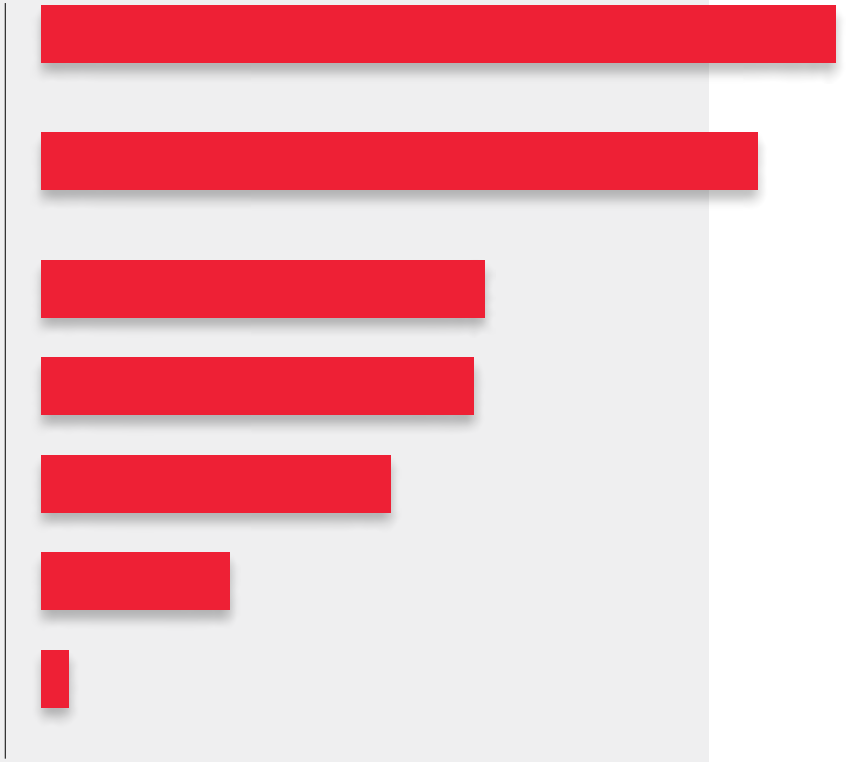
15% 

Loan fraud

12. Did your bank take any of the following steps to address fraud concerns in 2025?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs. Respondents were asked to select all that apply.

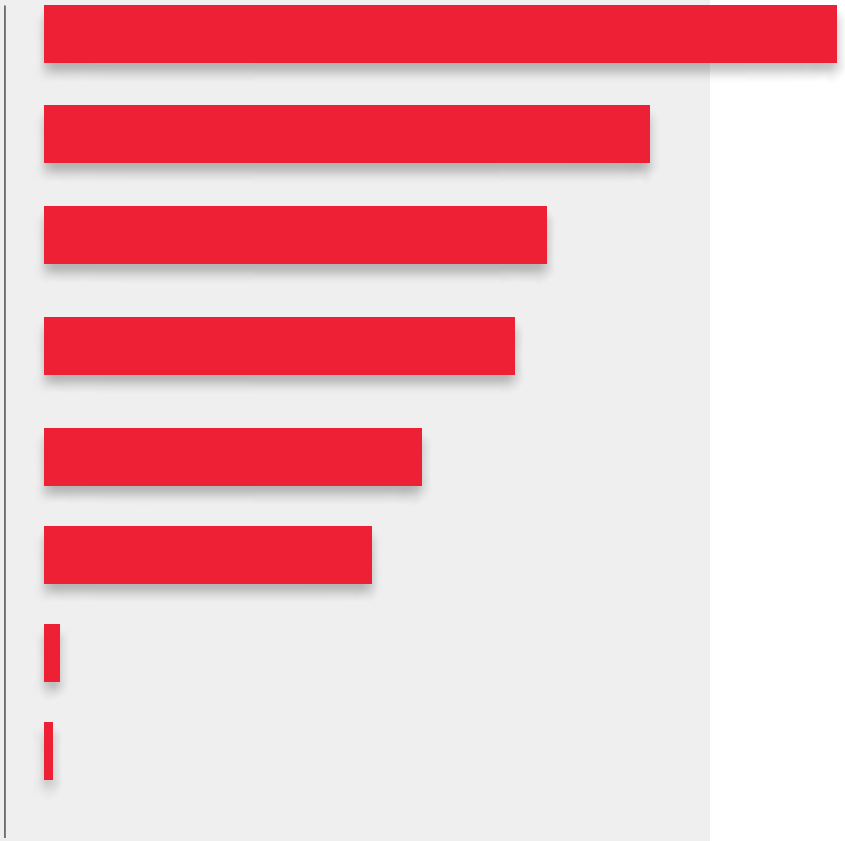
93%	Improved training for bank staff, including education about the latest scams/threats
84%	Regular communication to customers about relevant scams/threats
52%	Improved internal controls
51%	Improved board education
41%	Specific staff education on AI fraud and deepfake media
22%	Specific customer education on AI fraud and deepfake media
3%	Other



13. What metrics related to fraud and suspicious activity does management regularly share with the board?

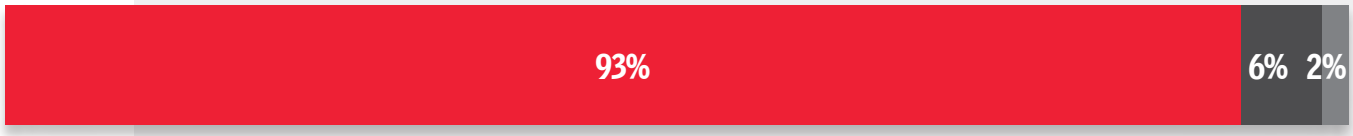
Question only asked of CEOs, board chairs and independent directors. Respondents were asked to select all that apply.

94%	Number of suspicious activity reports filed
71%	Types of fraud and scams reported by customers
59%	Number of fraud and scam attempts reported by customers
55%	Source of suspicious activity reports filed (i.e. specific customer types or geographies)
44%	Types of fraud and scam attempts on bank employees
38%	Number of fraud attempts on bank employees
2%	Other
1%	We don't receive information about any of these metrics



14. Do you feel this information is timely and clear enough to inform the board?

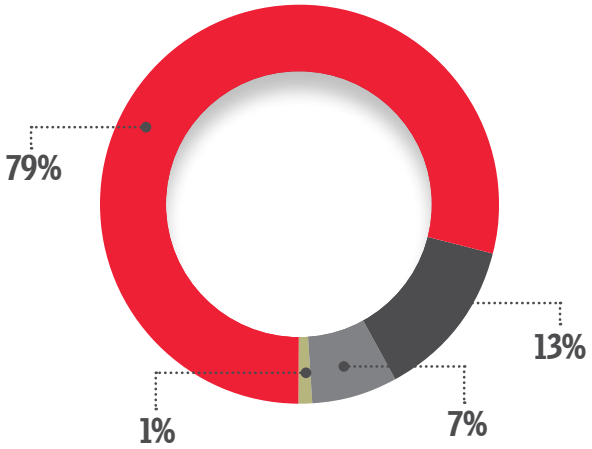
Question only asked of respondents who indicated that management regularly shares fraud metrics with the board. Numbers don't add up to 100% due to rounding.



- Yes
- No
- Unsure

15. Does the board take an active role in reviewing and approving the bank's cybersecurity strategy?

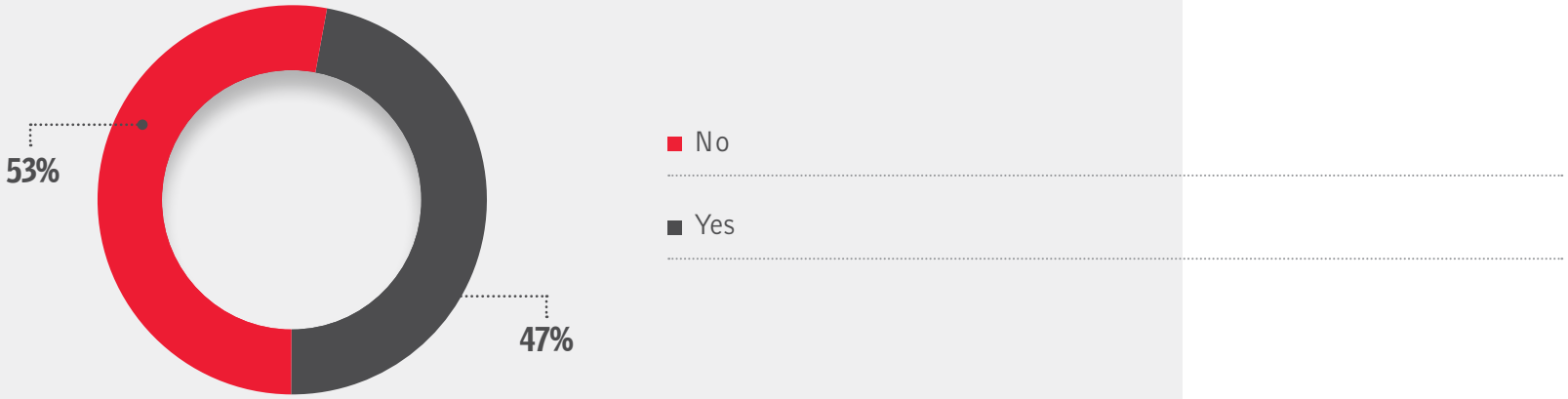
Question only asked of board chairs and independent directors.



- Yes, the board reviews and approves the cybersecurity strategy set by management.
- Yes, the board sets the cybersecurity strategy.
- No, the board has limited involvement in reviewing the cybersecurity strategy.
- Unsure

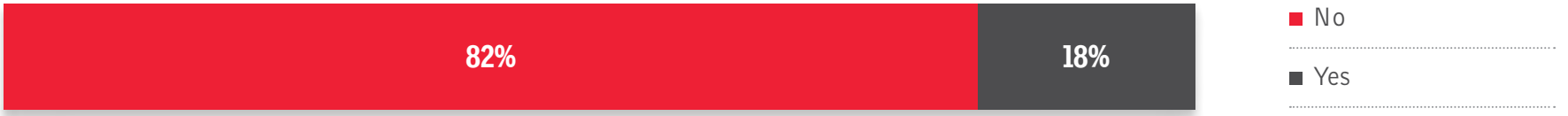
16. Did the board invite outside experts to talk about cybersecurity trends over the past 12 months?

Question only asked of board chairs and independent directors.



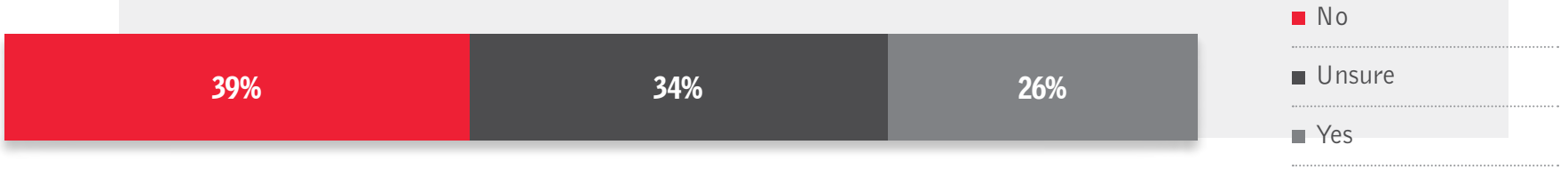
17. Did your bank add cybersecurity personnel in 2025?

Question not asked of board chairs, independent directors or chief credit officers.



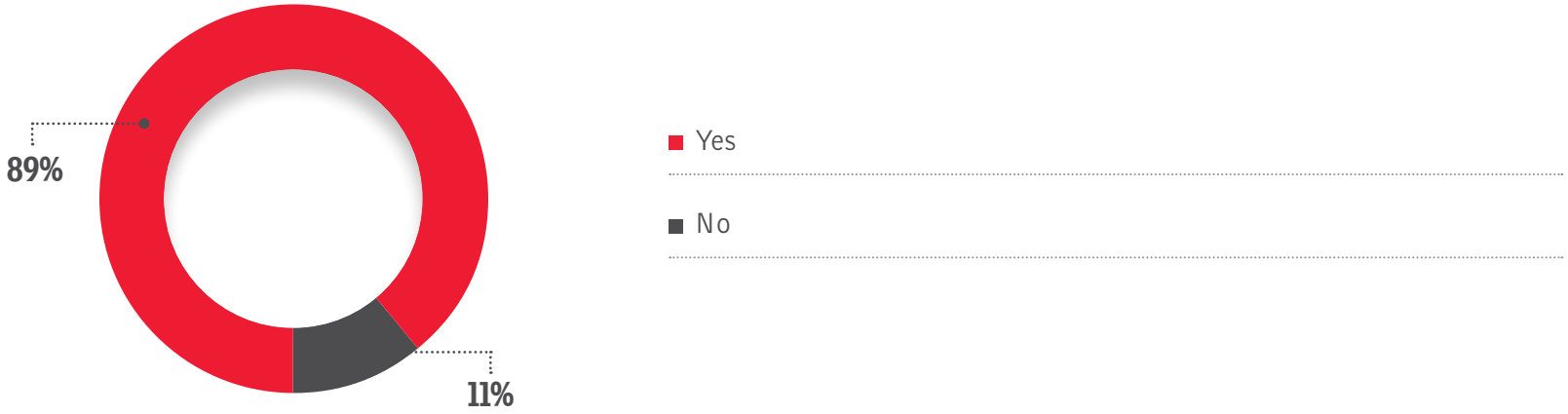
18. Have your bank's cybersecurity insurance premiums increased over the past 12 months?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs.



19. Has your bank conducted a tabletop exercise of its cybersecurity incident response plan within the past 12 months?

Question only asked of CEOs, CROs, CISOs, CIOs and CTOs.



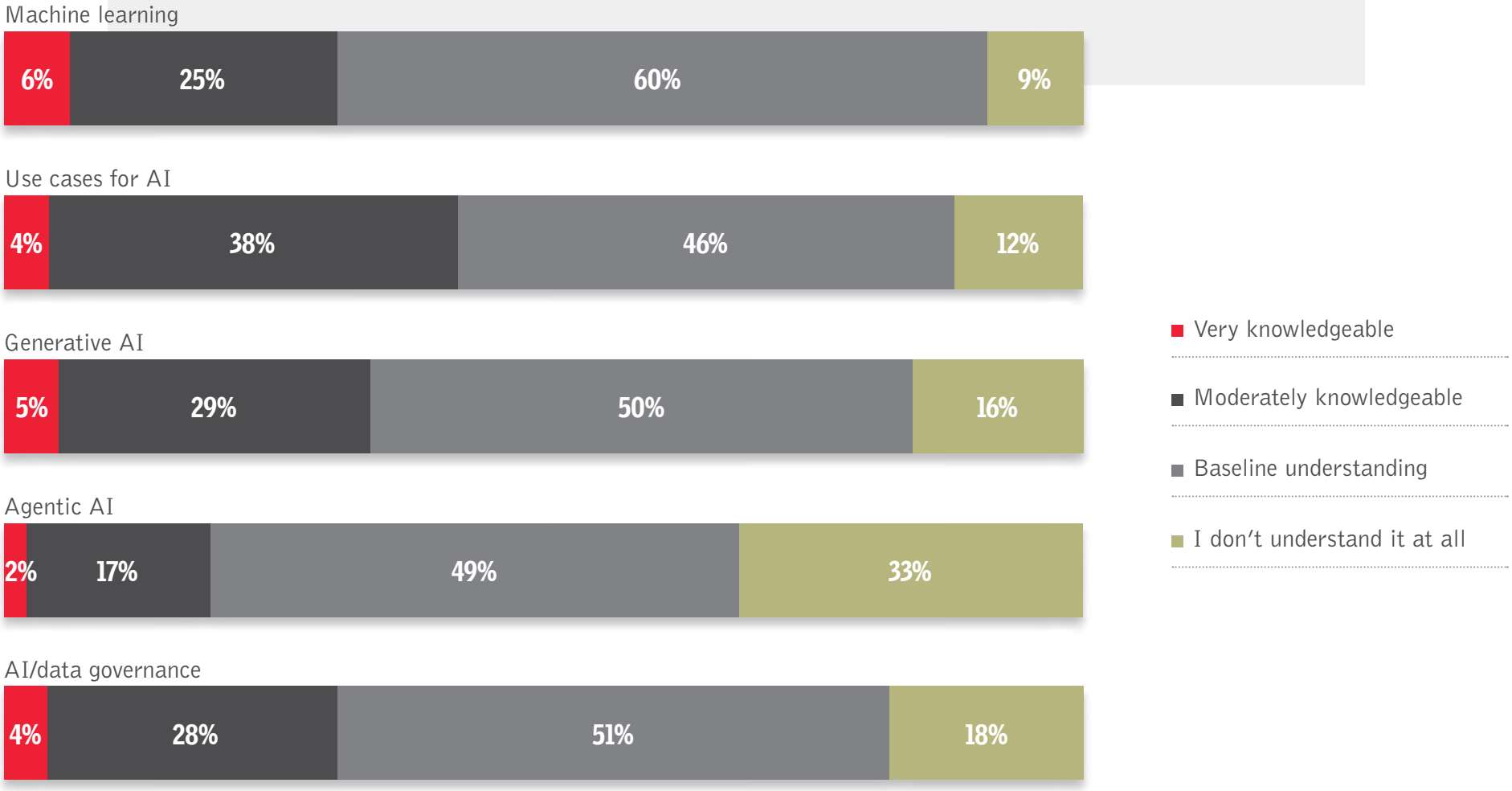
20. Did your bank find any gaps or vulnerabilities in any of the following areas during that tabletop exercise?

Question only asked of respondents who indicated their bank had conducted a tabletop exercise of its cybersecurity incident response plan in the past 12 months. Respondents were asked to select all that apply.

36%	Overreliance on one individual or function
35%	Internal communications
26%	No gaps were found
22%	Vendor vulnerabilities
21%	Overreliance on vendors for key functions such as data protection or risk management
14%	External communications
3%	Other
2%	Records retention

ARTIFICIAL INTELLIGENCE

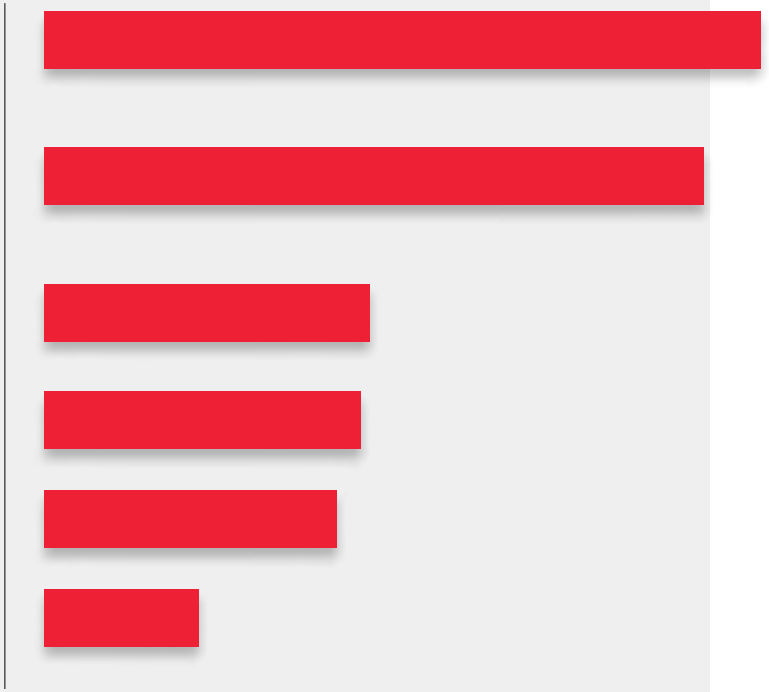
21. What is your knowledge level on various areas of artificial intelligence, including agentic AI?



22. What risks associated with AI are you most concerned about as they pertain to your bank?

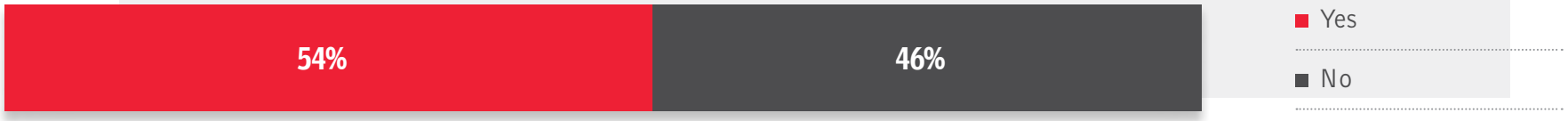
Question only asked of CEOs, CROs, CISOs, CIOs and CTOs. Respondents were asked to select no more than three responses.

84%	Increasingly sophisticated fraud and scams targeting our customers
77%	Increasingly sophisticated fraud and scams targeting our organization and/or employees
38%	Competitive threat from other financial institutions or nonbanks
37%	Data security risks from our own usage of AI
34%	Increased potential for third- and fourth-party risk
18%	Operational risk associated with our own use of AI technologies



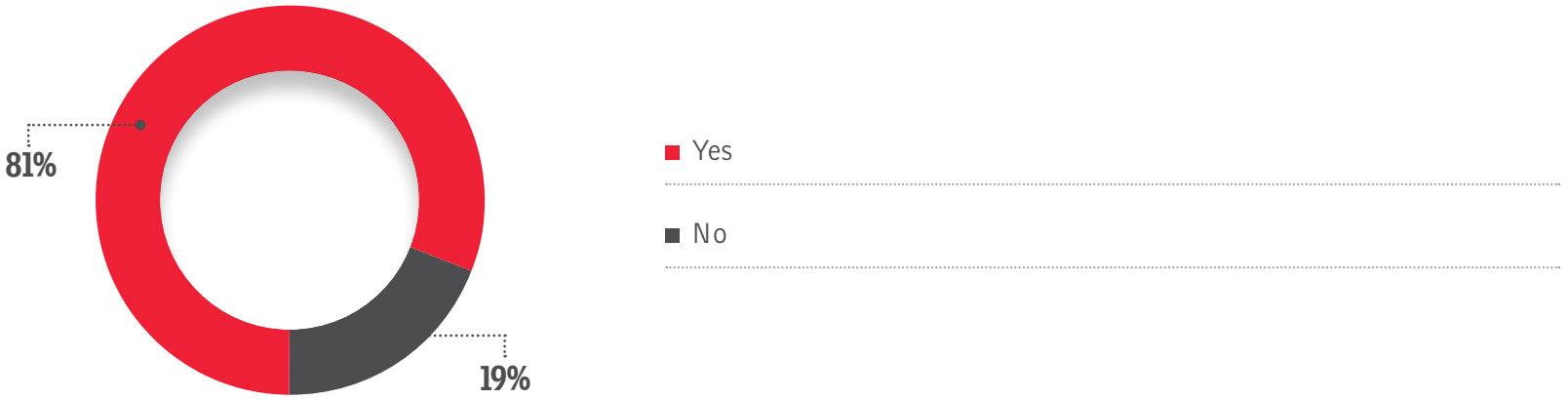
THE CHIEF RISK OFFICER

23. Does your bank have a chief risk officer?



24. Does your bank's chief risk officer report directly to the CEO?

Question only asked of respondents who indicated their bank has a chief risk officer.



25. Who reports to your bank's chief risk officer?

Question only asked of respondents who indicated their bank had a chief risk officer. Respondents were asked to select all that apply.

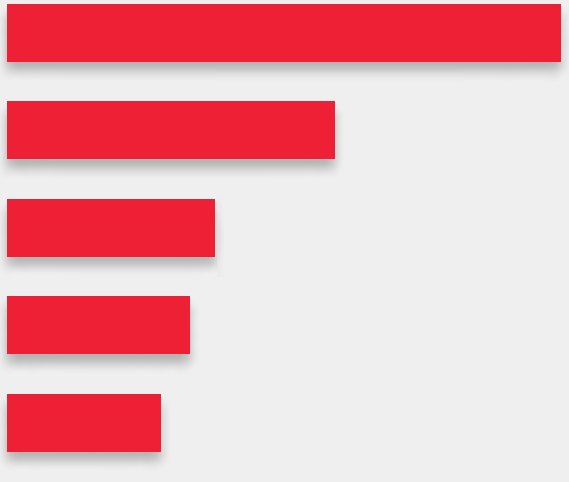
65% Chief compliance officer or equivalent

38% Chief information security officer or equivalent

24% Chief information officer or equivalent

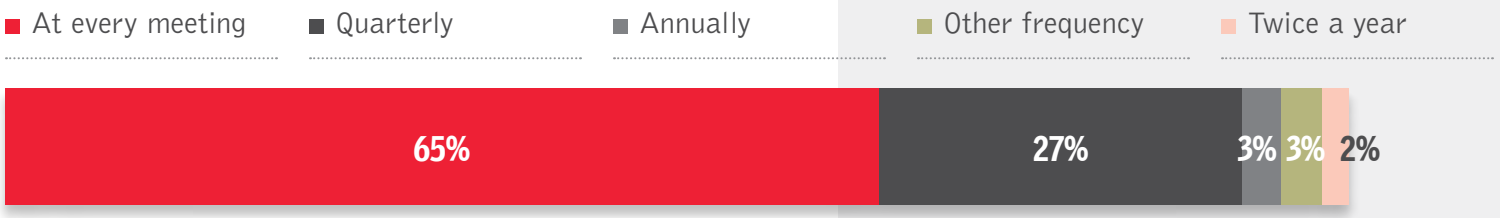
21% Chief credit officer or equivalent

18% None of the above



26. How often does your bank's chief risk officer interact with the board of directors?

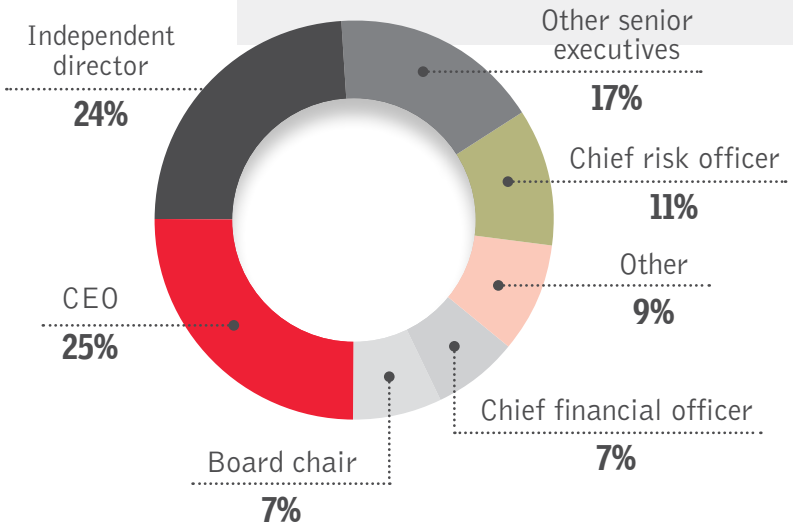
Question only asked of respondents who indicated their bank had a chief risk officer.



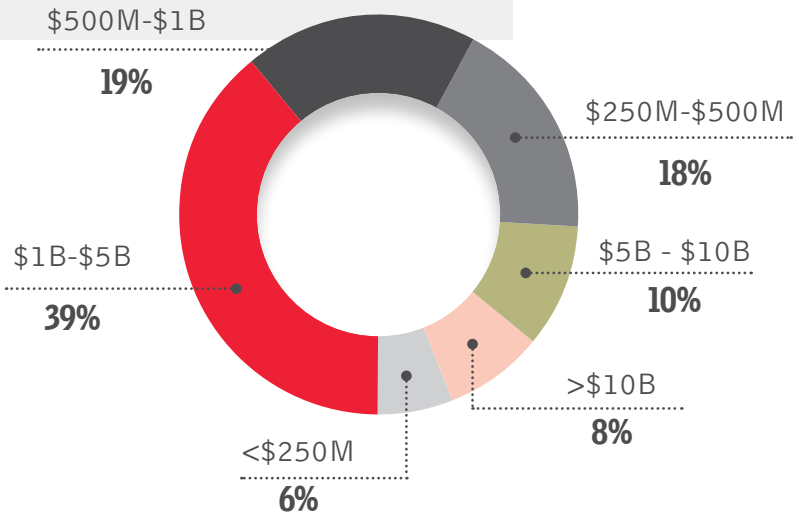
ABOUT THE SURVEY

Bank Director's 2026 Risk Survey, sponsored by Baker Tilly, surveyed 257 independent directors, chief executive officers, chief risk officers and other senior executives of U.S. banks below $100 billion of assets to gauge their concerns about key risks, including cybersecurity, fraud and credit risk. The survey was conducted in January 2026.

TITLE

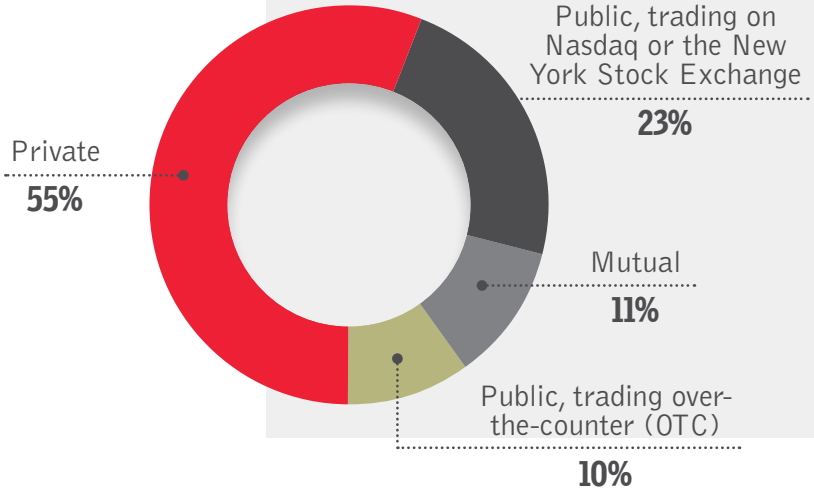


ASSET SIZE



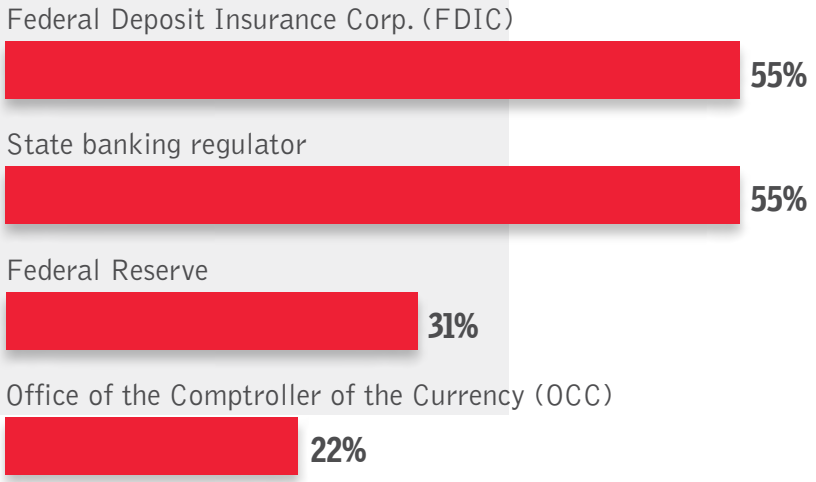
OWNERSHIP STRUCTURE

Numbers don't add up to 100% due to rounding.



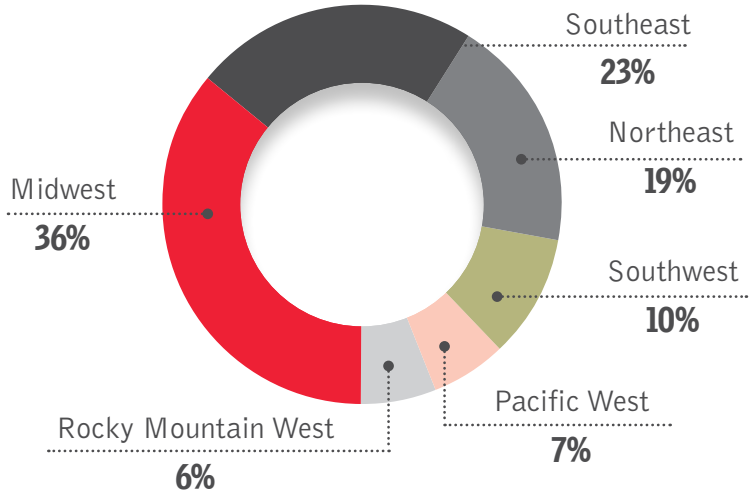
PRIMARY REGULATOR

Respondents were asked to select all that apply.



REGION*

Numbers don't add up to 100% due to rounding.



**Regions defined as follows: Midwest (IL, IN, IA, KS, MI, MN, MO, NE, ND, OH, SD, WI); Northeast (CT, ME, MA, NH, NJ, NY, PA, RI, VT); Pacific West (AK, CA, HI, OR, WA); Rocky Mountain West (CO, ID, MT, NV, UT, WY); Southeast (AL, AR, DE, DC, FL, GA, KY, LA, MD, MS, NC, SC, TN, VA, WV); Southwest (AZ, NM, OK, TX)*