

BankDirector
Strong Board. Strong Bank.

2017 Risk Practices Survey

MAR 2017 | RESEARCH

Sponsored by:

The FIS logo consists of the letters 'FIS' in a bold, green, sans-serif font. Above the letter 'I' are three small green dots.

TABLE OF CONTENTS

Executive Summary	3
Challenges & Concerns	4
Internal Controls	6
Cybersecurity	10
Vendor Management & Fintech	19
Regulatory Expectations	22
Risk & Cybersecurity Governance	26
About the Survey	30

BankDirector

About Bank Director

Since its inception in 1991, Bank Director has been a leading information resource for senior officers and directors of financial institutions. Chairmen, CEOs, CFOs, presidents and directors of banks and financial institutions turn to Bank Director to keep pace with the ever-changing landscape of the financial services industry. For more information about Bank Director, visit www.bankdirector.com.



About FIS

FIS (NYSE:FIS) is a global leader in financial services technology, with a focus on retail and institutional banking, payments, asset and wealth management, risk and compliance, consulting and outsourcing solutions. FIS serves over 20,000 financial institutions globally and is a Fortune 500 company and a member of the Standard & Poor's 500® Index. FIS' Risk, Information Security and Compliance (RISC) Solutions group provides clients a 360-degree solution set of products and services that enable enterprise risk management, enhance overall compliance programs and mitigate risk through a best practices-based model that ensures regulatory compliance proficiencies now and in the future. FIS was ranked #1 in the Chartis RiskTech 100® for 2016 and 2017. For more information, please visit www.fisglobal.com/risc.

EXECUTIVE SUMMARY

Conventional wisdom holds that bankers dislike the Dodd-Frank Act, but most financial leaders don't want Congress and President Trump to totally dismantle the law, according to Bank Director's 2017 Risk Practices Survey, which is sponsored by FIS.

Eighty-two percent of the 167 independent directors and senior executives of U.S. banks above \$500 million in assets surveyed by Bank Director in December 2016 and January 2017—following Trump's election but before his inauguration—expect to see regulatory relief this year. When asked about the aspects of Dodd-Frank that should be scaled back, respondents focus on the Consumer Financial Protection Bureau: 70 percent want to change the CFPB's structure, and 66 percent seek to scale back the bureau's considerable enforcement authority. Banks have invested a lot at this point to meet the requirements laid out by the law, and while the majority want to see Dodd-Frank changed in some way, few—just 20 percent—believe it should be repealed entirely. A surprising 7 percent—all from banks under \$5 billion in assets—say it should remain unchanged.

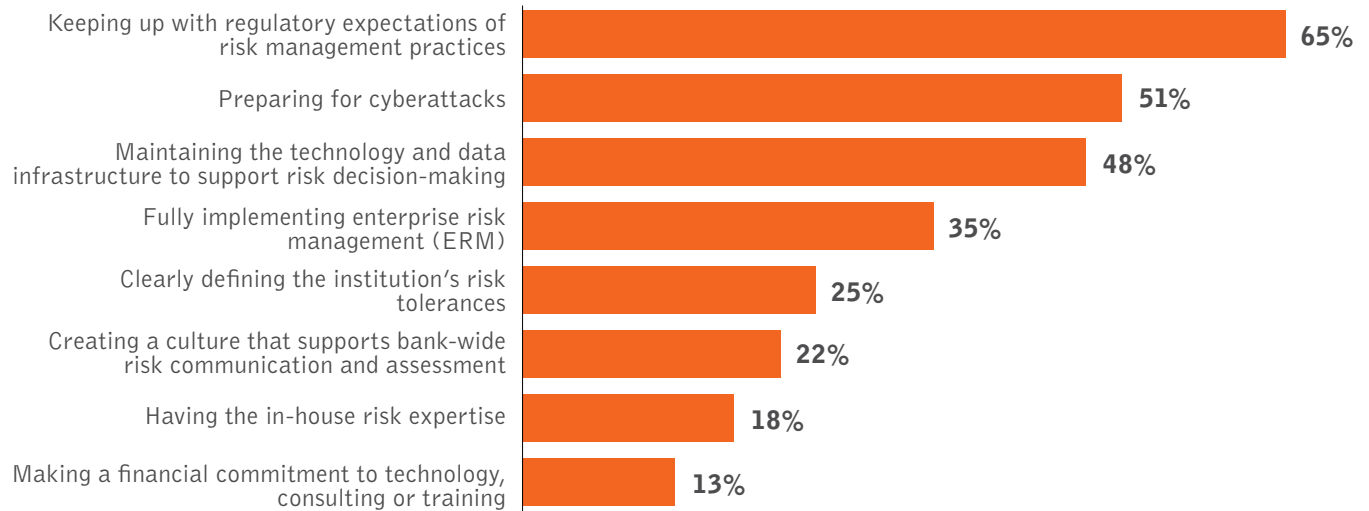
Key Findings:

- Forty-eight percent would like to see the Durbin amendment restrictions on debit interchange fees at banks with \$10 billion or more in assets scaled back. Home Mortgage Disclosure Act rules, for 43 percent, and qualified mortgage rules, for 39 percent, are also identified as regulatory pain points.
- Eighty-four percent believe that bank regulators are open to the implementation of innovative products and services through relationships between banks and third-party financial technology firms.
- Eighty-three percent believe that lowering corporate tax rates would be the best way to encourage economic growth in the U.S.
- Preparing for cyberattacks continues to be another key challenge for the industry, according to 51 percent of respondents. Financial institutions have made considerable improvements to cybersecurity programs, including investments in technology to better detect and deter cyber threats (82 percent), improved training for bank staff (81 percent) and increased focus on cybersecurity at the board level (80 percent).
- Employee susceptibility to phishing or other types of social engineering schemes is the area in which the majority of respondents think the bank is least prepared for a cyberattack or data breach, at 57 percent.
- Seventy-seven percent say their board has discussed the Wells Fargo cross-selling scandal and its potential impact on the bank. Of these, 42 percent have evaluated their bank's incentive compensation programs, and the same number evaluated the bank's retail sales culture or goals. Eight percent eliminated cross-selling programs.

CHALLENGES & CONCERNS

1. What are your bank's three biggest risk management challenges?

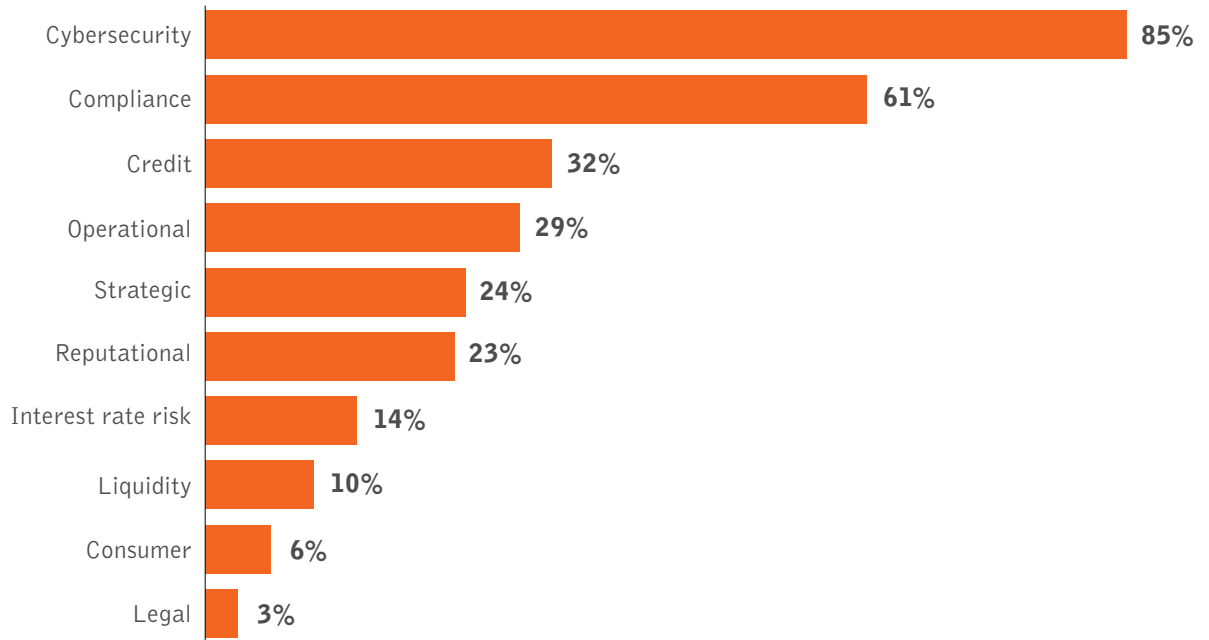
Respondents were allowed to select no more than three. Chief information officers (CIOs), chief technology officers (CTOs) and chief information security officers (CISOs) were not asked to respond to this question.



Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Keeping up with regulatory expectations of risk management practices	82%	62%	61%	67%	65%
Preparing for cyberattacks	55%	38%	59%	44%	51%
Maintaining the technology and data infrastructure to support risk decision-making	55%	67%	42%	44%	48%
Fully implementing enterprise risk management (ERM)	9%	33%	38%	40%	35%
Clearly defining the institution's risk tolerances	9%	29%	21%	33%	25%
Creating a culture that supports bank-wide risk communication and assessment	36%	10%	24%	21%	22%
Having the in-house risk expertise	-	5%	21%	26%	18%
Making a financial commitment to technology, consulting or training	27%	24%	9%	12%	13%

2. With respect to your bank, which three risk categories are you most concerned about?

Respondents were allowed to select no more than three. CIOs, CTOs and CISOs were not asked to respond to this question

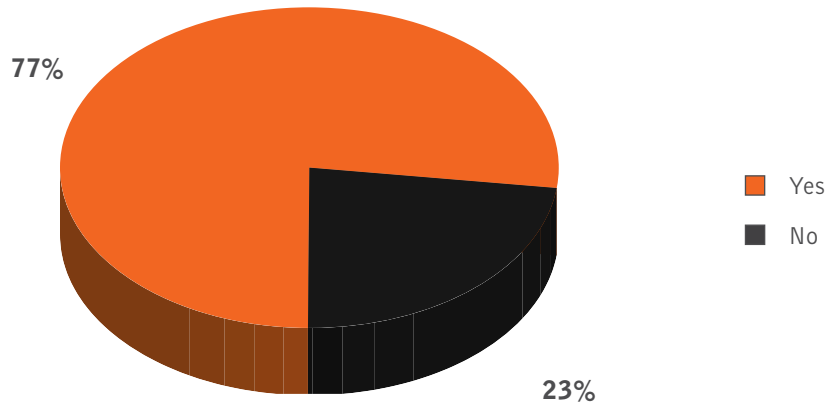


Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Cybersecurity	91%	90%	81%	86%	85%
Compliance	91%	52%	59%	60%	61%
Credit	36%	24%	38%	26%	32%
Operational	18%	48%	22%	33%	29%
Strategic	18%	19%	31%	19%	24%
Reputational	36%	14%	24%	23%	23%
Interest rate risk	-	14%	15%	16%	14%
Liquidity	-	10%	6%	19%	10%
Consumer	-	5%	7%	5%	6%
Legal	-	-	1%	7%	3%

INTERNAL CONTROLS

3. Wells Fargo made headlines in 2016 following the discovery that its aggressive sales culture, focused on cross-selling, led thousands of employees to open 2 million unauthorized accounts. Has your board discussed the Wells Fargo case and its potential impact on your bank?

CIOs, CTOs and CISOs were not asked to respond to this question.



Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	91%	95%	70%	77%	77%
No	9%	5%	30%	23%	23%

4. Has this discussion resulted in examining or changing policies, procedures or internal controls? In what way?

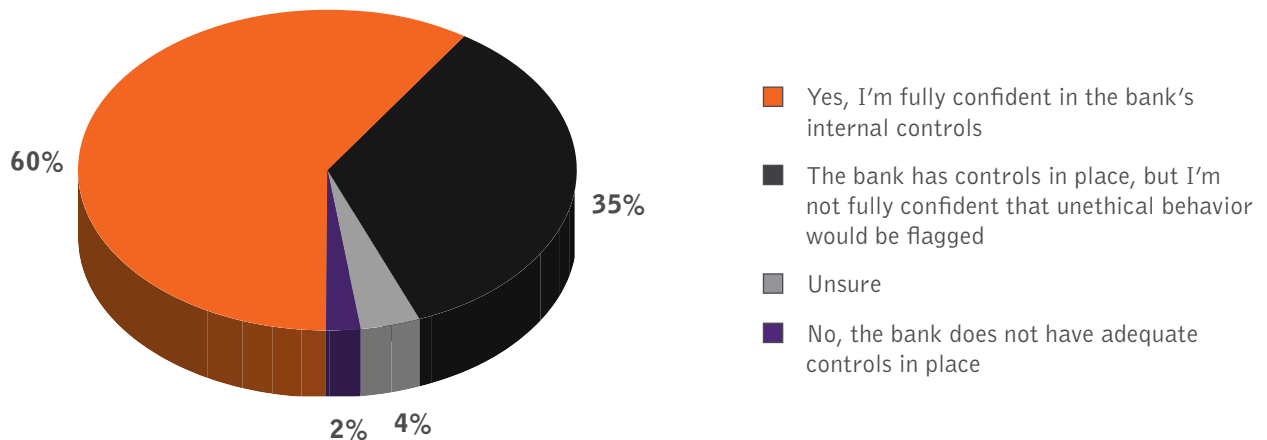
Question was only asked of respondents whose board has discussed the Wells Fargo case and its potential impact. Respondents were asked to select all that apply. CIOs, CTOs and CISOs were not asked to respond to this question.



Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
The bank has made no changes	50%	30%	52%	48%	47%
Evaluated the bank's incentive compensation programs	30%	65%	39%	35%	42%
Evaluated the bank's retail sales culture and/or goals	30%	65%	30%	48%	42%
Evaluated how the bank handles ethical/fraud complaints	10%	25%	15%	16%	17%
Strengthened/created ways for employees to identify and communicate unethical behavior	-	-	15%	10%	9%
Eliminated cross-selling programs	10%	10%	7%	10%	8%
Changed incentive compensation plans for retail employees	10%	10%	4%	10%	7%
Eliminated incentive compensation plans for retail employees	-	5%	7%	10%	7%
Changed retail sales goals at the bank	-	5%	4%	13%	7%
Other	10%	-	7%	-	4%
Changed the way the bank handles ethical/fraud complaints	-	5%	4%	-	3%
Changed the bank's retail sales culture	-	5%	2%	-	2%

5. Does your bank have internal controls in place that you are confident would flag unethical behavior?

CIOs, CTOs and CISOs were not asked to respond to this question.

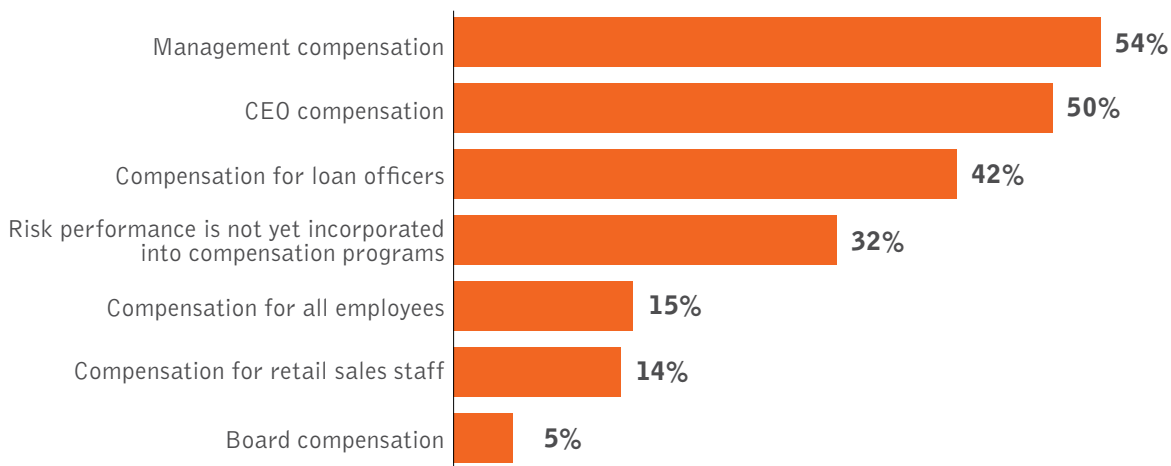


Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes, I'm fully confident in the bank's internal controls	64%	67%	58%	57%	60%
The bank has controls in place, but I'm not fully confident that unethical behavior would be flagged	36%	24%	39%	33%	35%
Unsure	-	10%	1%	5%	4%
No, the bank does not have adequate controls in place	-	-	1%	5%	2%

Title	CEO	CRO	Chairman/ Director	Other officer/Other	Total
Yes, I'm fully confident in the bank's internal controls	79%	50%	59%	52%	60%
The bank has controls in place, but I'm not fully confident that unethical behavior would be flagged	-	50%	37%	44%	35%
Unsure	11%	-	2%	4%	4%
No, the bank does not have adequate controls in place	11%	-	1%	-	2%

6. In which areas of the bank is risk performance incorporated into compensation programs, to reward employees who stay within the bank's risk parameters?

Respondents were asked to select all that apply. CIOs, CTOs and CISOs were not asked to respond to this question.

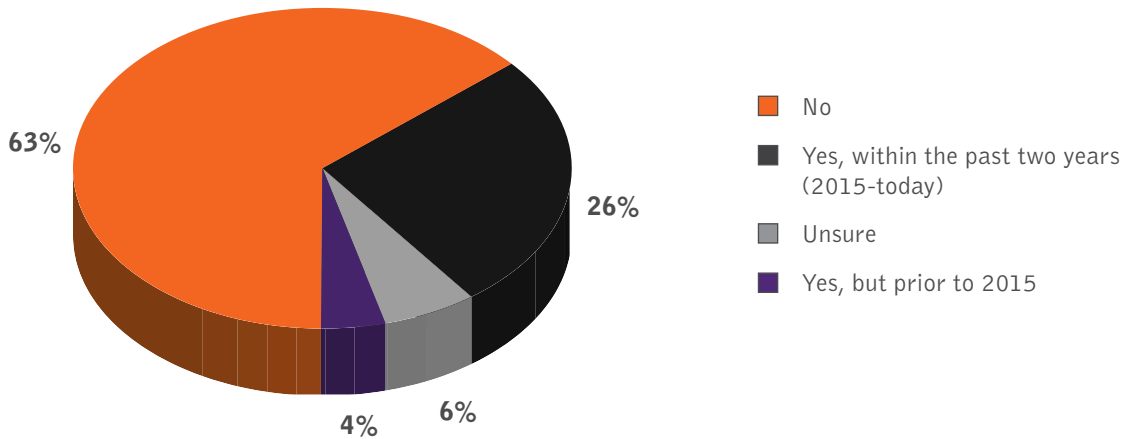


Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Management compensation	64%	60%	51%	54%	54%
CEO compensation	64%	50%	46%	51%	50%
Compensation for loan officers	55%	55%	35%	41%	42%
Risk performance is not yet incorporated into compensation programs	27%	25%	32%	37%	32%
Compensation for all employees	18%	20%	15%	12%	15%
Compensation for retail sales staff	18%	10%	20%	5%	14%
Board compensation	-	5%	5%	7%	5%

CYBERSECURITY

7. Has your bank experienced a data breach or other cyberattack?

**Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
No	22%	48%	68%	73%	63%
Yes, within the past two years (2015-today)	33%	35%	26%	20%	26%
Unsure	33%	13%	2%	5%	6%
Yes, but prior to 2015	11%	4%	5%	2%	4%

8. Over the past two years (2015-today), in what areas has your bank made improvements to its cybersecurity program?

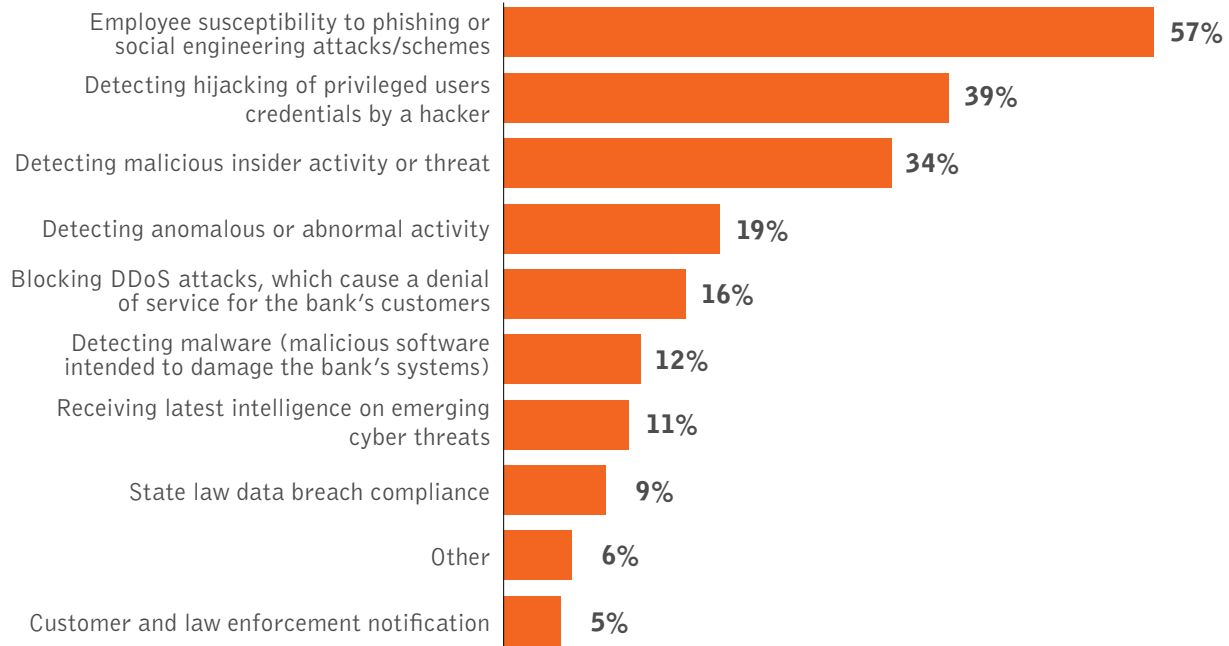
Respondents were asked to select all that apply.



Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Invested in technology to better detect and deter cyber threats and intrusions	100%	91%	75%	84%	82%
Improved training for bank staff	70%	83%	80%	84%	81%
Increased focus on cybersecurity at the board level	90%	87%	75%	82%	80%
Improved internal controls related to information security	80%	61%	74%	82%	75%
Improved and tested cyber-incident management and response plan	90%	78%	74%	70%	75%
Increased investment in cybersecurity personnel	90%	70%	63%	50%	62%
Improved intelligence on emerging cyber threats	70%	74%	51%	52%	56%

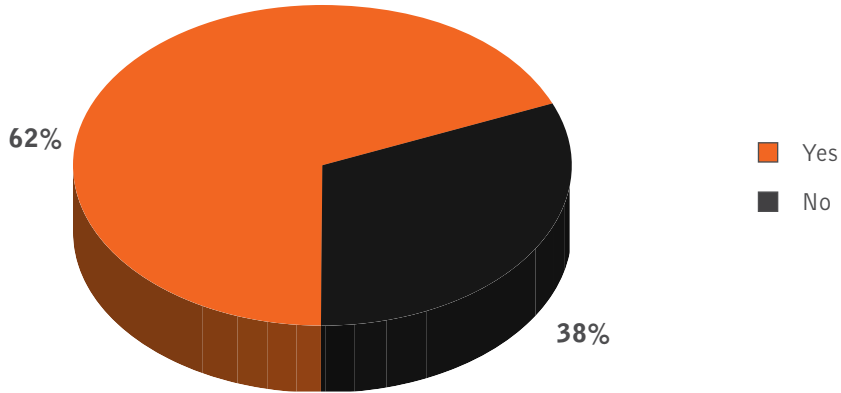
9. When it comes to preparing for a cyberattack or data breach, in what areas do you think the bank is least prepared?

Respondents were asked to select all that apply. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Employee susceptibility to phishing or social engineering attacks/schemes	67%	57%	60%	50%	57%
Detecting hijacking of privileged users credentials by a hacker	33%	33%	38%	43%	39%
Detecting malicious insider activity or threat	44%	24%	40%	29%	34%
Detecting anomalous or abnormal activity	44%	14%	10%	29%	19%
Blocking DDoS attacks, which cause a denial of service for the bank's customers	-	5%	11%	31%	16%
Detecting malware (malicious software intended to damage the bank's systems)	33%	-	10%	17%	12%
Receiving latest intelligence on emerging cyber threats	11%	10%	14%	7%	11%
State law data breach compliance	-	19%	5%	12%	9%
Other	11%	14%	6%	-	6%
Customer and law enforcement notification	11%	-	3%	10%	5%

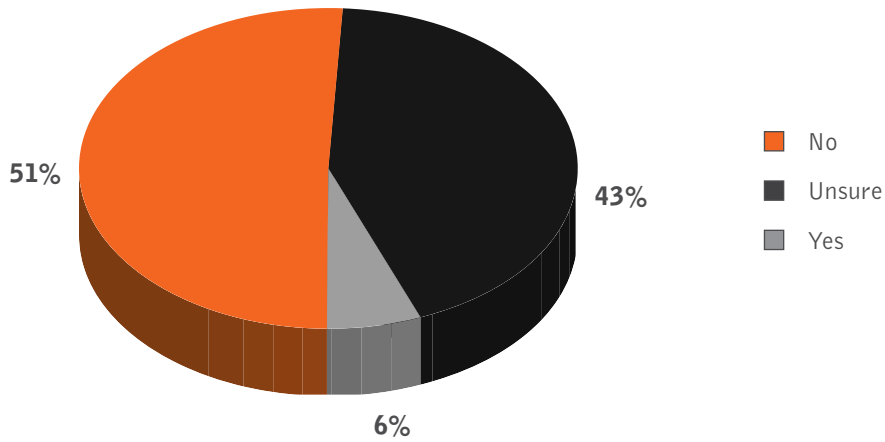
10. Does your bank employ a full-time chief information security officer (CISO)?



Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	90%	82%	69%	35%	62%
No	10%	18%	31%	65%	38%

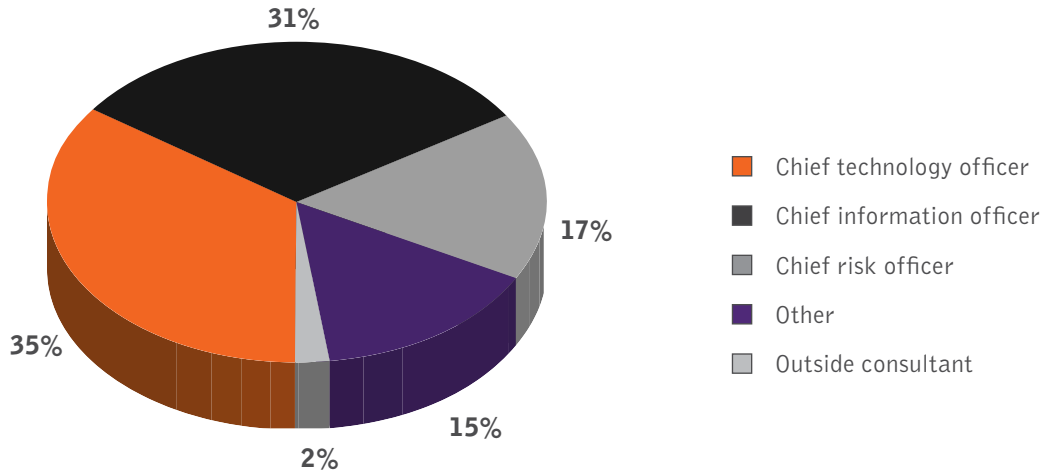
11. Does your bank plan to employ a full-time CISO by the end of 2017?

Question was only asked of respondents whose bank does not employ a full-time CISO.

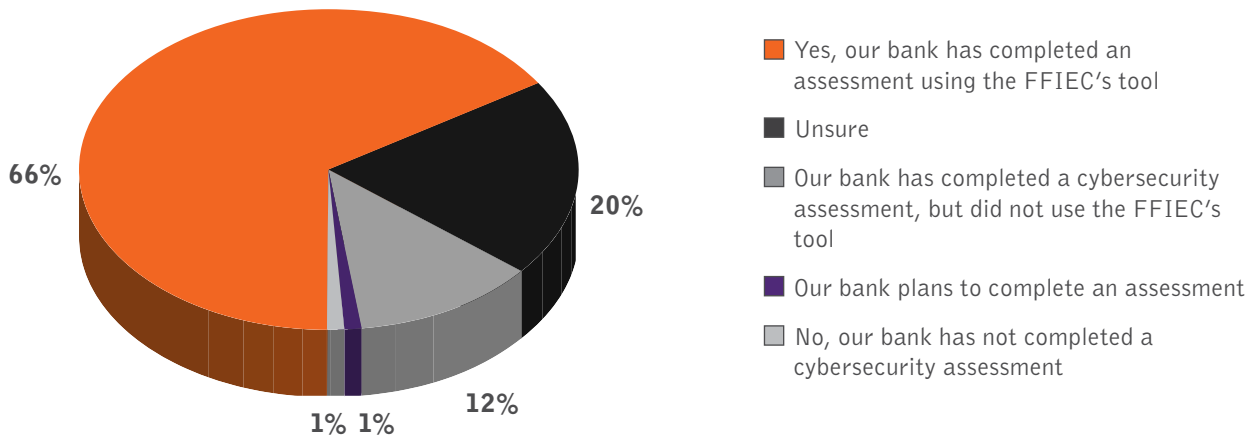


12. Who currently handles information security/cybersecurity at your bank?

Question was only asked of respondents whose bank does not employ a full-time CISO.



13. Has your bank conducted an assessment using the FFIEC Cybersecurity Assessment Tool?

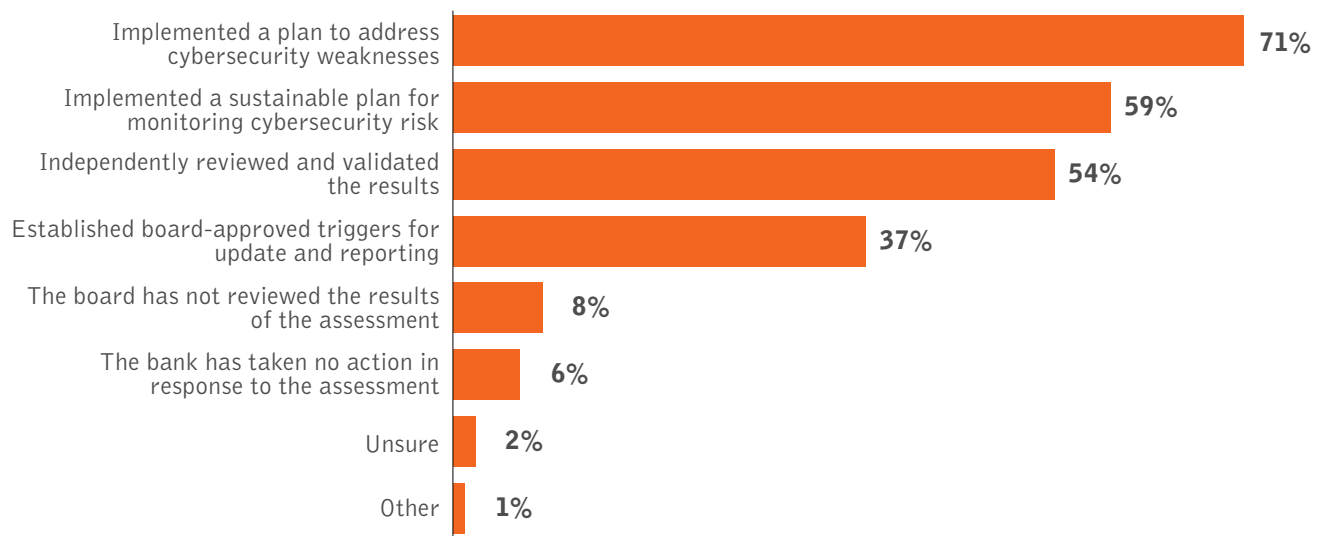


Bank Asset Size	>\$10B	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes, our bank has completed an assessment using the FFIEC's tool	60%	70%	61%	73%	66%
Unsure	10%	26%	28%	7%	20%
Our bank has completed a cybersecurity assessment, but did not use the FFIEC's tool	30%	4%	9%	16%	12%
Our bank plans to complete an assessment	-	-	2%	2%	1%
No, our bank has not completed a cybersecurity assessment	-	-	-	2%	1%

Does your bank employ a CISO?	Yes	No	Total
Yes, our bank has completed an assessment using the FFIEC's tool	73%	55%	66%
Unsure	15%	27%	20%
Our bank has completed a cybersecurity assessment, but did not use the FFIEC's tool	9%	16%	12%
Our bank plans to complete an assessment	2%	-	1%
No, our bank has not completed a cybersecurity assessment	-	2%	1%

14. Has the bank done any of the following in response to the completed cybersecurity assessment?

Question was only asked of respondents whose bank has completed a cybersecurity assessment, either the FFIEC's or an alternate assessment. Respondents were asked to select all that apply. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Implemented a plan to address cybersecurity weaknesses	89%	81%	67%	67%	71%
Implemented a sustainable plan for monitoring cybersecurity risk	67%	62%	62%	51%	59%
Independently reviewed and validated the results	44%	56%	44%	67%	54%
Established board-approved triggers for update and reporting	33%	31%	44%	31%	37%
The board has not reviewed the results of the assessment	-	12%	4%	13%	8%
The bank has taken no action in response to the assessment	-	-	9%	8%	6%
Unsure	11%	-	-	3%	2%
Other	-	-	-	3%	1%

15. Based on the cybersecurity assessment completed by the bank, how mature is the cybersecurity program in each of the following areas?

Question was only asked of respondents whose bank has completed an FFIEC cybersecurity assessment. Respondents were asked to evaluate each factor based on the FFIEC's maturity scale, with "baseline" indicating the lowest level of maturity and "innovative" indicating the highest maturity level. *Indicates a base count of less than 10 within a category.

Cybersecurity risk management/oversight					
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Baseline (lowest)	17%	13%	17%	32%	21%
Evolving	-	27%	20%	25%	21%
Intermediate	-	33%	34%	25%	29%
Advanced	67%	20%	23%	18%	24%
Innovative (highest)	17%	7%	6%	-	5%

Threat intelligence/ collaboration					
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Baseline (lowest)	-	7%	18%	29%	18%
Evolving	17%	33%	26%	43%	33%
Intermediate	-	40%	35%	21%	29%
Advanced	50%	13%	21%	7%	17%
Innovative (highest)	33%	7%	-	-	4%

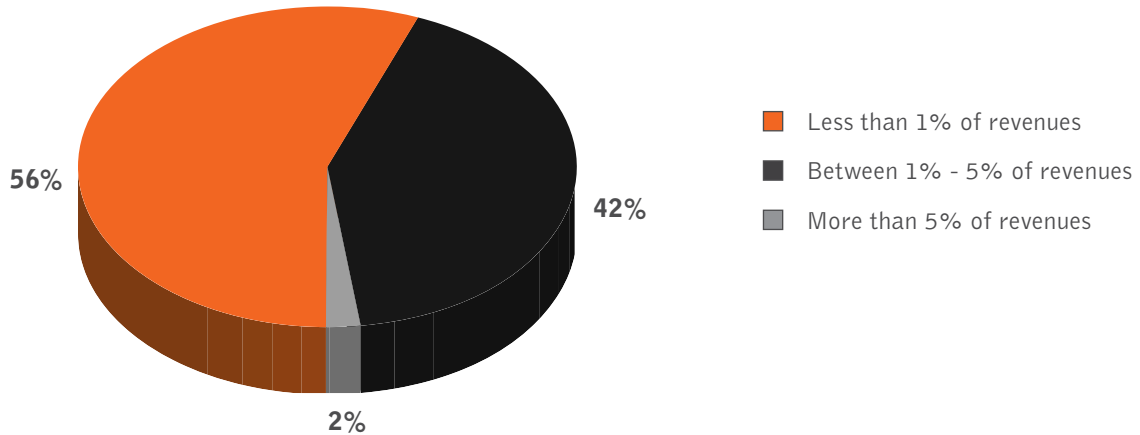
Cybersecurity controls					
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Baseline (lowest)	17%	20%	17%	30%	22%
Evolving	-	20%	23%	22%	20%
Intermediate	17%	40%	31%	30%	31%
Advanced	50%	13%	29%	19%	24%
Innovative (highest)	17%	7%	-	-	2%

External dependency management					
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Baseline (lowest)	-	13%	18%	32%	20%
Evolving	17%	27%	24%	18%	22%
Intermediate	33%	47%	29%	36%	35%
Advanced	33%	7%	26%	14%	19%
Innovative (highest)	17%	7%	3%	-	4%

Cyber incident management/response					
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Baseline (lowest)	-	20%	15%	38%	22%
Evolving	17%	20%	33%	8%	21%
Intermediate	33%	33%	24%	35%	30%
Advanced	33%	20%	27%	19%	24%
Innovative (highest)	17%	7%	-	-	2%

16. How large was your bank’s cybersecurity budget for fiscal year 2016?

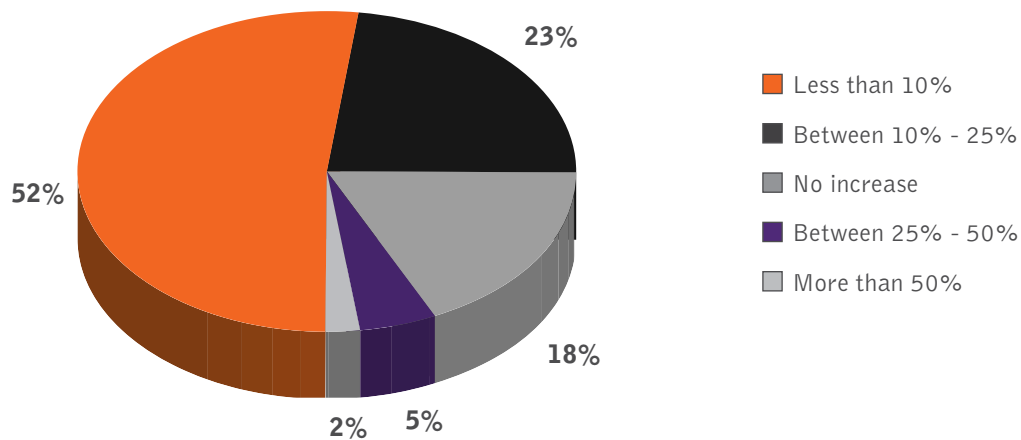
**Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Less than 1% of revenues	62%	47%	57%	58%	56%
Between 1% - 5% of revenues	38%	53%	43%	37%	42%
More than 5% of revenues	-	-	-	5%	2%

17. How much has your bank’s cybersecurity budget increased for FY 2017?

**Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Less than 10%	50%	41%	53%	57%	52%
Between 10% - 25%	38%	18%	28%	14%	23%
No increase	12%	12%	13%	30%	18%
Between 25% - 50%	-	29%	2%	-	5%
More than 50%	-	-	4%	-	2%

18. How much has your bank budgeted for cybersecurity expenses, including personnel and technology, for FY 2017?

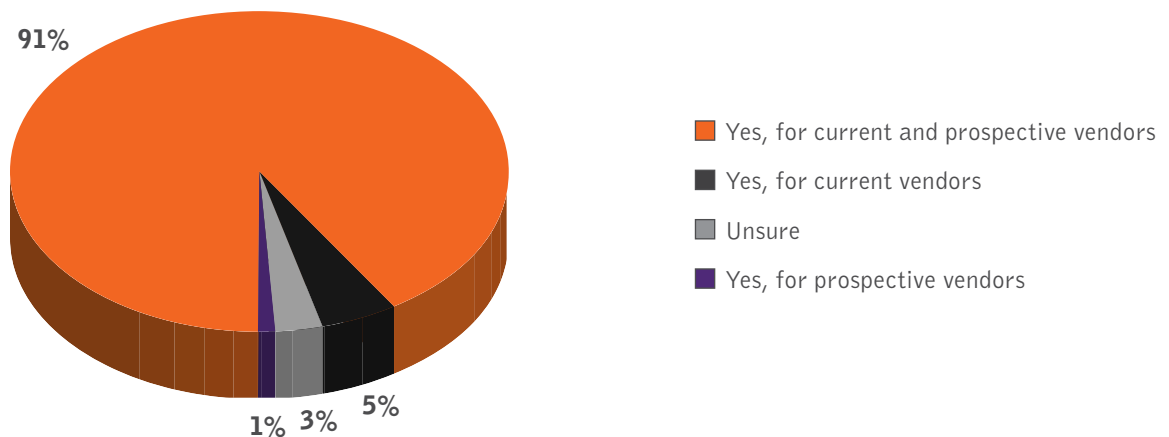
Median value reported.

\$200,000

VENDOR MANAGEMENT & FINTECH

19. Does your bank have policies and procedures in place to assess and monitor the risk posed by current and prospective vendors?

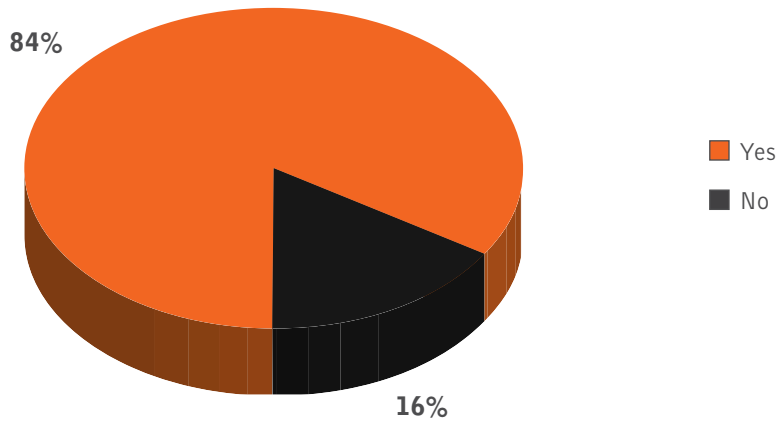
CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes, for current and prospective vendors	100%	77%	92%	95%	91%
Yes, for current vendors	-	14%	5%	2%	5%
Unsure	-	9%	3%	-	3%
Yes, for prospective vendors	-	-	-	2%	1%

20. In your opinion, are your bank’s regulators currently open to the implementation of innovative products and services at your bank through relationships with third-party financial technology firms?

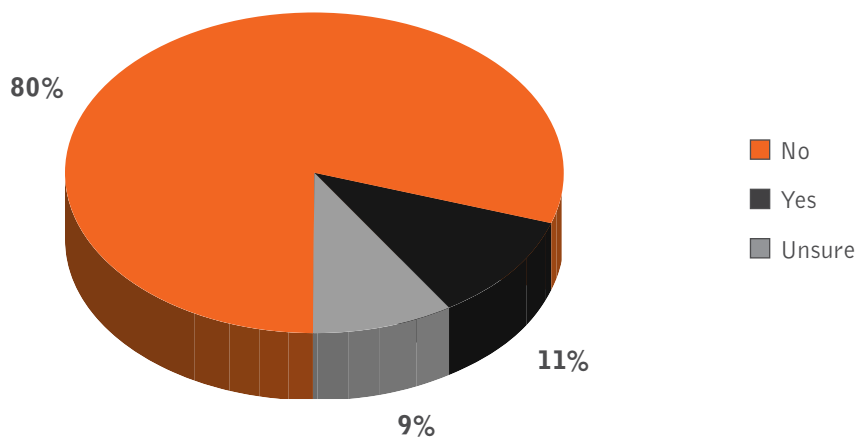
*CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	89%	90%	84%	80%	84%
No	11%	10%	16%	20%	16%

21. Has the bank received negative comments from its regulators due to a partnership with a financial technology firm within the past two years?

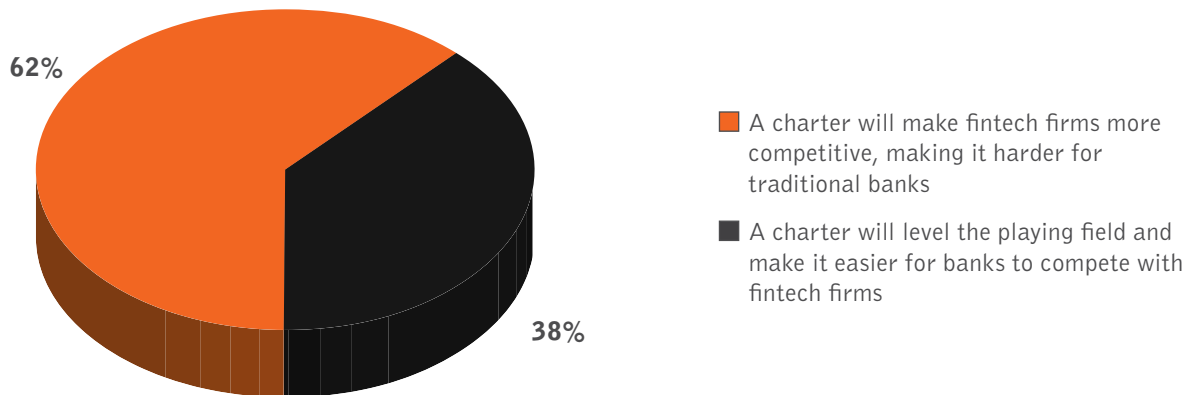
*CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
No	67%	68%	81%	88%	80%
Yes	11%	9%	14%	7%	11%
Unsure	22%	23%	5%	5%	9%

22. The Office of the Comptroller of the Currency has announced its intentions to grant limited purpose banking charters to financial technology firms. How do you believe this will impact the banking industry?

*CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.*



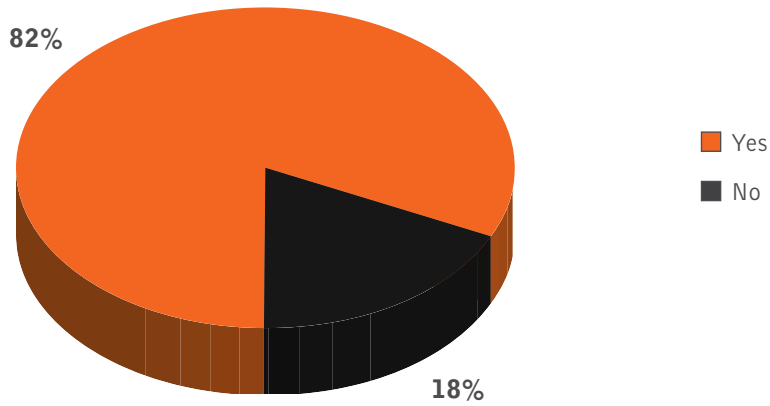
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
A charter will make fintech firms more competitive, making it harder for traditional banks	67%	65%	64%	58%	62%
A charter will level the playing field and make it easier for banks to compete with fintech firms	33%	35%	36%	42%	38%

Title	CEO	CRO	CIO/CTO*	Chairman/ Director	Other officer/ Other	Total
A charter will make fintech firms more competitive, making it harder for traditional banks	47%	43%	50%	69%	71%	62%
A charter will level the playing field and make it easier for banks to compete with fintech firms	53%	57%	50%	31%	29%	38%

REGULATORY EXPECTATIONS

23. Given a Republican administration and Congress, do you believe that the banking industry will see regulatory relief by the end of 2017?

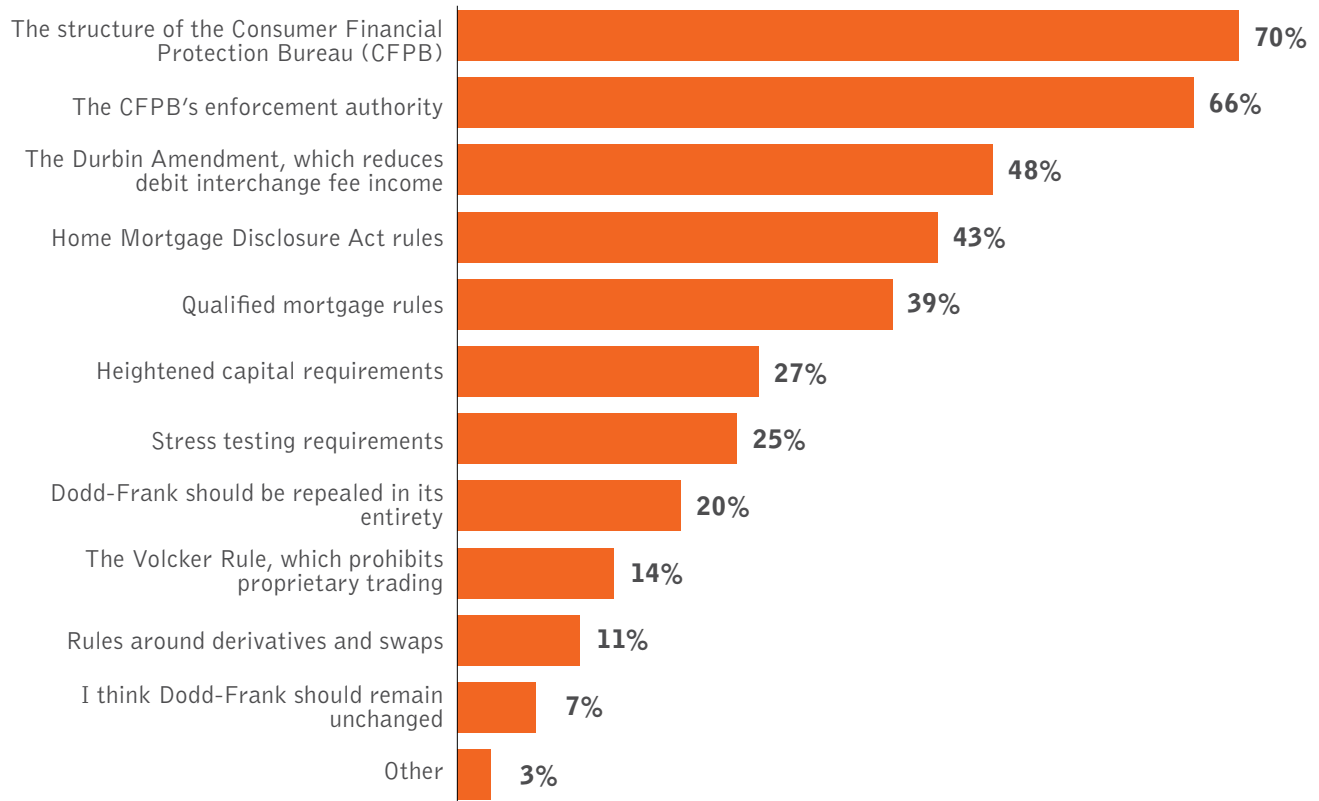
*CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	89%	84%	75%	89%	82%
No	11%	16%	25%	11%	18%

24. What aspects of the Dodd-Frank Act do you believe should be scaled back?

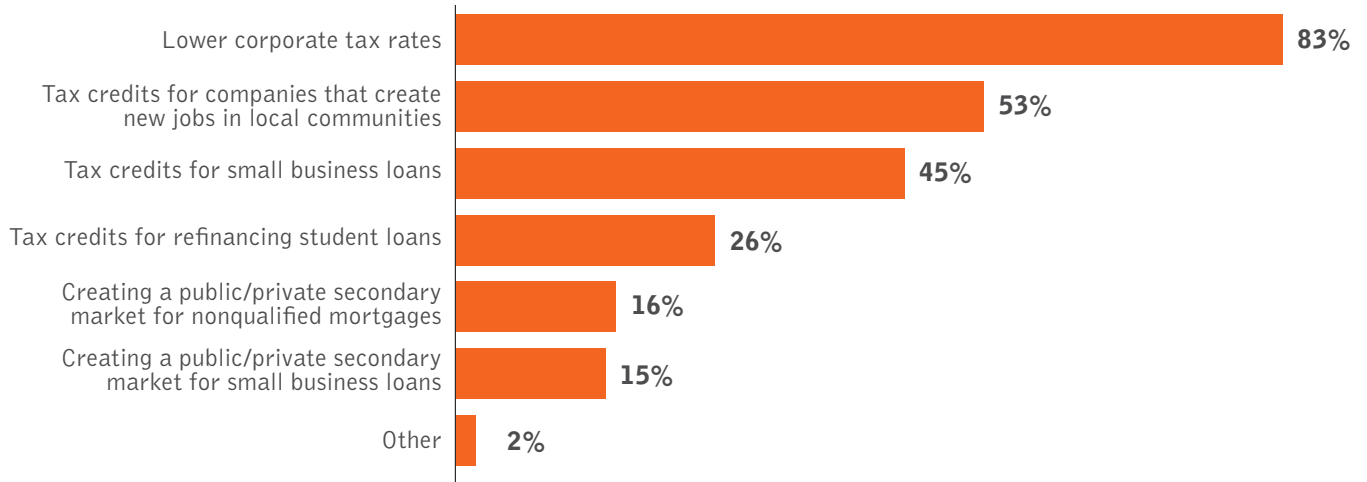
Respondents were asked to select all that apply. CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
The structure of the Consumer Financial Protection Bureau (CFPB)	67%	84%	65%	73%	70%
The CFPB's enforcement authority	44%	84%	65%	62%	66%
The Durbin Amendment, which reduces debit interchange fee income	56%	84%	42%	35%	48%
Home Mortgage Disclosure Act rules	33%	32%	49%	43%	43%
Qualified mortgage rules	33%	26%	44%	38%	39%
Heightened capital requirements	33%	26%	26%	27%	27%
Stress testing requirements	67%	32%	21%	16%	25%
Dodd-Frank should be repealed in its entirety	33%	32%	18%	16%	20%
The Volcker Rule, which prohibits proprietary trading	22%	26%	9%	14%	14%
Rules around derivatives and swaps	44%	5%	9%	11%	11%
I think Dodd-Frank should remain unchanged	-	-	12%	5%	7%
Other	-	5%	4%	3%	3%

25. Which regulatory reforms would best encourage growth for the U.S. economy and/or the banking industry?

Respondents were asked to select all that apply. CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.



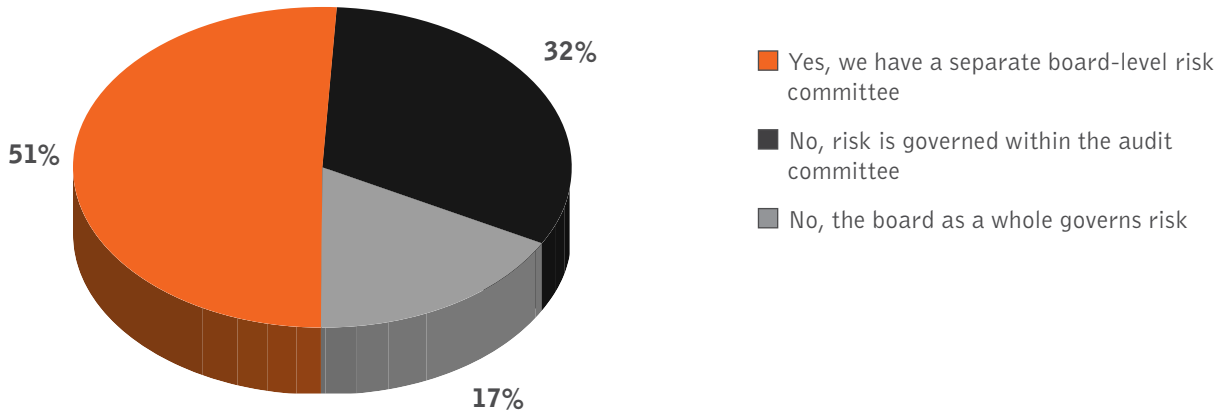
Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Lower corporate tax rates	89%	95%	84%	72%	83%
Tax credits for companies that create new jobs in local communities	56%	65%	54%	44%	53%
Tax credits for small business loans	11%	55%	40%	56%	45%
Tax credits for refinancing student loans	22%	25%	28%	25%	26%
Creating a public/private secondary market for nonqualified mortgages	-	25%	16%	14%	16%
Creating a public/private secondary market for small business loans	22%	10%	14%	17%	15%
Other	-	-	-	6%	2%

Title	CEO	CRO	Chairman/ Director	Other officer/Other	Total
Lower corporate tax rates	94%	64%	86%	77%	83%
Tax credits for companies that create new jobs in local communities	31%	43%	53%	77%	53%
Tax credits for small business loans	31%	36%	47%	55%	45%
Tax credits for refinancing student loans	12%	14%	33%	23%	26%
Creating a public/private secondary market for nonqualified mortgages	12%	36%	13%	14%	16%
Creating a public/private secondary market for small business loans	6%	7%	16%	23%	15%
Other	6%	-	1%	-	2%

RISK & CYBERSECURITY GOVERNANCE

26. Does the board have a separate committee exclusively dedicated to risk governance?

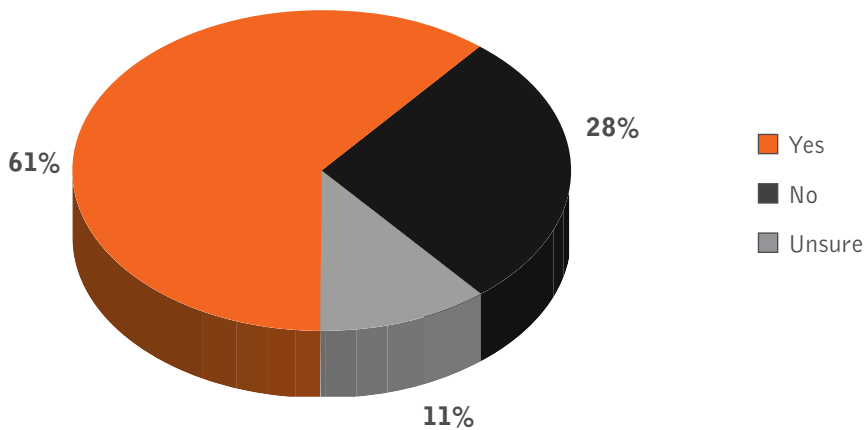
CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes, we have a separate board-level risk committee	100%	80%	55%	16%	51%
No, risk is governed within the audit committee	-	15%	32%	49%	32%
No, the board as a whole governs risk	-	5%	12%	35%	17%

27. Does your board have at least one member who you would consider to be an expert on risk as relates to financial institutions?

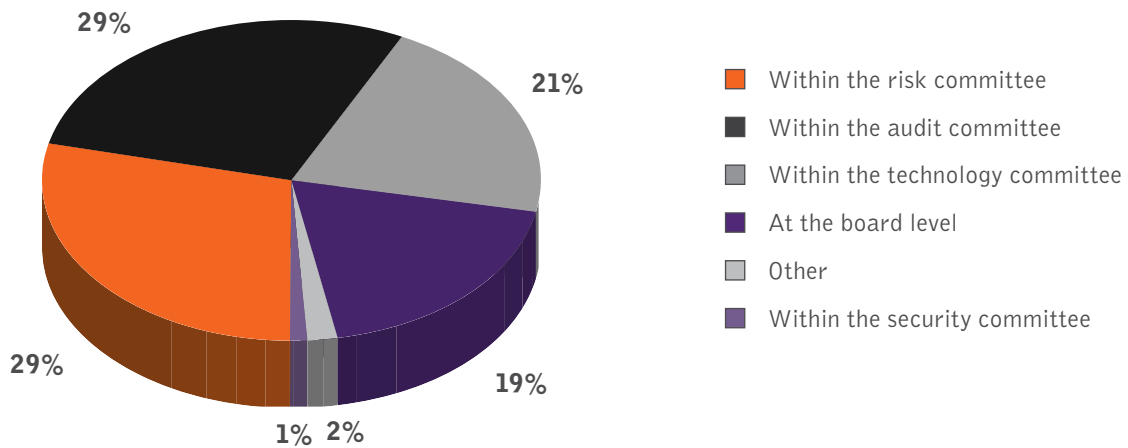
CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	56%	75%	57%	62%	61%
No	33%	-	36%	30%	28%
Unsure	11%	25%	7%	8%	11%

28. How does the board primarily handle cybersecurity governance?

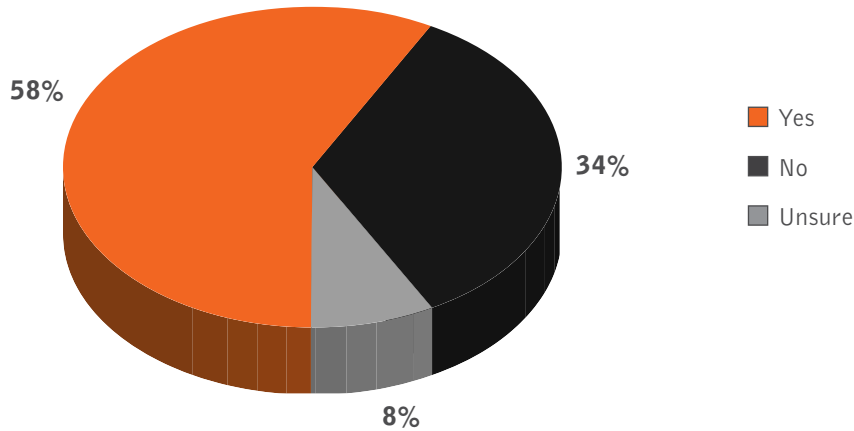
*CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.*



Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Within the risk committee	67%	45%	32%	5%	29%
Within the audit committee	-	25%	21%	49%	29%
Within the technology committee	33%	10%	21%	24%	21%
At the board level	-	15%	21%	22%	19%
Other	-	5%	2%	-	2%
Within the security committee	-	-	2%	-	1%

29. Does the committee tasked with cybersecurity governance review cybersecurity at every committee meeting?

Question was only asked of respondents whose bank handles cybersecurity within a committee. CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.

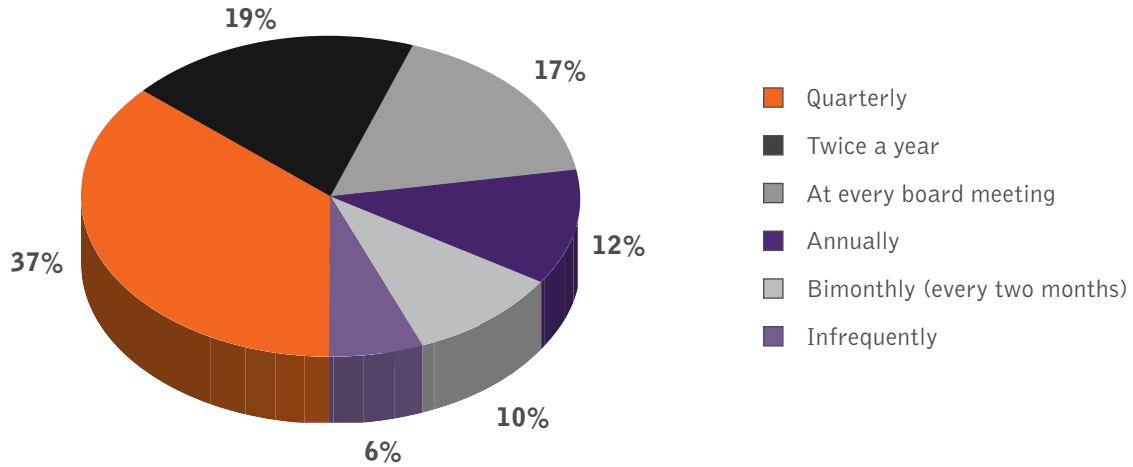


Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Yes	56%	53%	57%	62%	58%
No	22%	35%	39%	31%	34%
Unsure	22%	12%	5%	7%	8%

Cybersecurity Governance	Risk committee	Audit committee	Technology committee	Total
Yes	63%	51%	58%	58%
No	26%	46%	31%	34%
Unsure	11%	3%	12%	8%

30. How frequently does the board review cybersecurity?

CIOs, CTOs and CISOs were not asked to respond to this question. *Indicates a base count of less than 10 within a category.

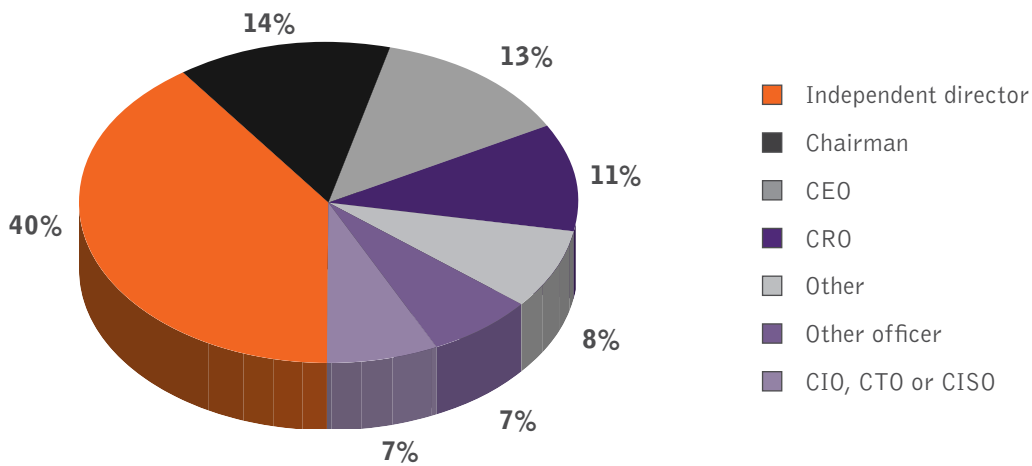


Bank Asset Size	>\$10B*	\$5B - \$10B	\$1B - \$5B	<\$1B	Total
Quarterly	22%	45%	40%	32%	37%
Twice a year	11%	25%	16%	22%	19%
At every board meeting	22%	10%	16%	19%	17%
Annually	11%	5%	11%	16%	12%
Bimonthly (every two months)	11%	5%	11%	11%	10%
Infrequently	22%	10%	5%	-	6%

ABOUT THE SURVEY

Bank Director’s 2017 Risk Practices Survey, sponsored by FIS, surveyed 167 board members, chief executive officers, risk officers and other senior executives of U.S. banks above \$500 million in assets about issues related to risk management and cybersecurity that are currently impacting the banking industry. Questions posed to CISOs were limited to cybersecurity, and CIOs and CTOs only shared their views on cybersecurity, vendor management and fintech. The survey was conducted in December 2016 and January 2017. Forty-five percent of respondents represent banks between \$1 billion and \$5 billion in assets, and 23 percent banks above \$5 billion. Independent directors and chairmen account for 54 percent of responses.

Title Breakdown



Bank Asset Size

