Bank Director

Strong Board. Strong Bank.

2016 Risk Practices Survey

MAR 2016 | RESEARCH

Sponsored by:

TABLE OF CONTENTS

Bank Director

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.

FIS

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. FIS is a Fortune 500 company, a member of the Standard & Poor's 500® Index and is ranked #1 on the Chartis 2016 RiskTech 100®. 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, information security, enhance overall compliance programs and mitigate risk through a best practices-based model that ensures regulatory compliance proficiencies now and in the future. For more information, please visit www.fisglobal.com/risc.

EXECUTIVE SUMMARY

For 77 percent of the bank executives and board members responding to Bank Director's 2016 Risk Practices Survey, sponsored by FIS, cybersecurity remains their top concern, for the second year in a row. More than half indicate that preparing for cyberattacks is one of their organization's biggest risk management challenges. While these concerns aren't new, respondents this year indicate a shift in how their boards and executives are addressing the threat. Unfortunately, the fact remains that many banks still aren't doing enough to protect themselves—and their customers.

Just 18 percent indicate their bank has experienced a data breach, but it's important to note that these breaches were almost as likely to occur at a smaller, $500 million asset institution as at a larger institution above $10 billion. Cybersecurity can no longer be dismissed as merely a "big bank" concern.

In addition to identifying cybersecurity practices within the industry, the online survey asked 161 independent directors and chairmen, chief risk officers, chief executive officers and other senior executives of U.S. banks above $500 million in assets to weigh in on their bank's risk governance, culture and infrastructure. The survey was conducted in January.

Compared to last year's survey results, more respondents indicate their board reviews cybersecurity at every board meeting, at 34 percent compared to 18 percent last year. While this shift represents a significant increase in board-level attention to cyberthreats compared to last year, these institutions remain the exception rather than the rule.

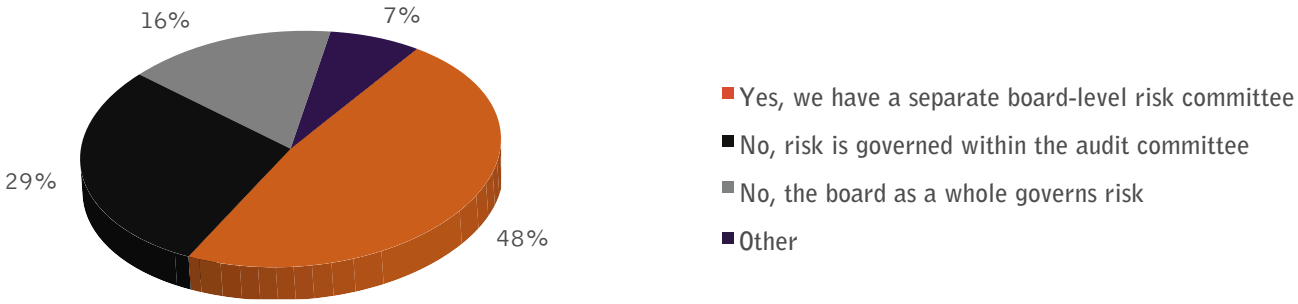
Many banks have yet to fully utilize the Cybersecurity Assessment Tool, developed by the Federal Financial Institutions Examination Council and made available to banks in 2015 "to help institutions identify their risks and determine their cybersecurity maturity." Sixty-two percent of survey respondents indicate their bank has used the tool and completed an assessment. However, just 39 percent have validated the results, and 18 percent established board-approved triggers for update and reporting. All three prudential regulators—the Federal Reserve, the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corp.—now use the tool in exams, regardless of the bank's size. Several states have mandated its use as well.

Key Findings:

- Seventy-eight percent indicate that their bank employs a full-time chief information security officer, up from 64 percent in last year's survey.
- Almost half report that the bank has a chief risk officer exclusively focused on risk, while 37 percent have a risk officer that is also focused on other areas of the bank.
- Fifty-four percent of respondents who indicate that the bank has a CRO also say the board never meets with that individual.
- Responses indicate a low level of board engagement with the chief risk officer: Just 21 percent indicate the CRO's performance is reviewed, and compensation determined by, the board or a board committee.
- Forty-eight percent of respondents govern risk within a separate, board-level risk committee, and 65 percent have at least one director who is considered to be a risk expert.
- Forty-five percent indicate that risk performance is not incorporated into their bank's compensation programs.
- Just 55 percent indicate their bank has a risk appetite statement, which defines the acceptable amount of risk for an organization.

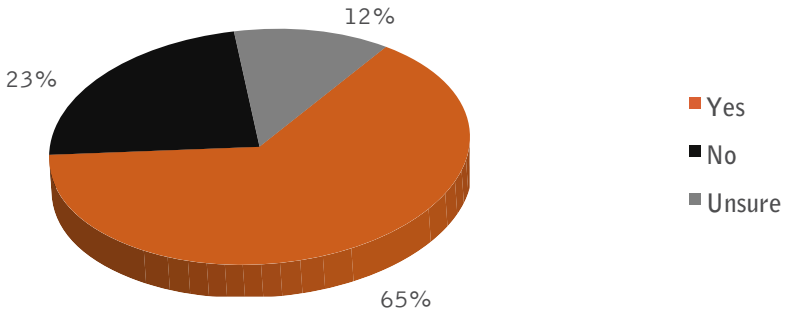
RISK GOVERNANCE & OVERSIGHT

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



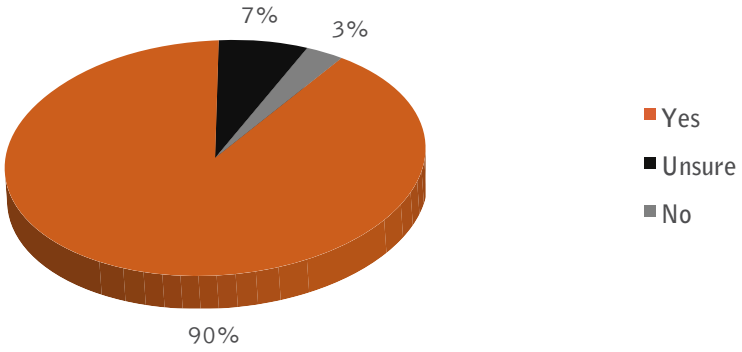
Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes, we have a separate board-level risk committee	89%	78%	44%	18%	48%
No, risk is governed within the audit committee	5%	19%	30%	44%	29%
No, the board as a whole governs risk	-	4%	14%	33%	16%
Other	5%	-	11%	4%	7%

2. Does your board have a least one member that you would consider to be an expert on risk as relates to financial institutions?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes	89%	89%	58%	50%	65%
No	-	11%	26%	35%	23%
Unsure	11%	-	16%	15%	12%

3. Do you feel that your bank's current governance structure effectively addresses the risks facing your institution?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes	100%	100%	87%	85%	90%
Unsure	-	-	9%	10%	7%
No	-	-	4%	5%	3%

Which board committee governs risk?	Separate risk committee	Audit committee	Entire board	Total
Yes	94%	87%	79%	90%
Unsure	4%	7%	17%	7%
No	1%	7%	4%	3%

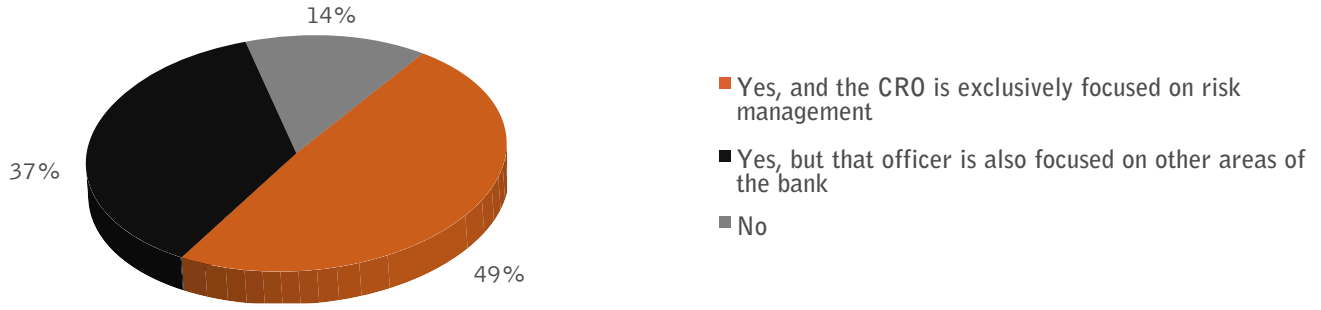
Does the board have a risk expert?	Board has a risk expert	Board doesn't have a risk expert	Unsure	Total
Yes	98%	74%	79%	90%
Unsure	1%	20%	11%	7%
No	1%	6%	11%	3%

4. Concerning the committee that governs risk, what is that committee's responsibility for risk governance?
Respondents were asked to select all that apply

Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Review enterprise risk assessment	100%	93%	81%	79%	85%
Approve risk policies	83%	89%	76%	71%	78%
Oversee the bank's risk management framework	67%	78%	72%	71%	72%
Compliance with the risk management program's policies and procedures	78%	78%	69%	66%	71%
Oversee risk dashboard reporting	83%	89%	69%	47%	69%
Establish risk appetite	94%	81%	60%	50%	66%
Review the bank's cybersecurity plan	78%	59%	65%	58%	64%
Review stress testing results	94%	59%	54%	61%	62%
Review strategic plan and risk mitigation strategies	83%	63%	50%	53%	57%
Review compensation risk	39%	41%	38%	29%	36%
Other	6%	-	9%	-	5%
Unsure	-	4%	1%	5%	3%

Which board committee governs risk?	Separate risk committee	Audit committee	Entire board	Total
Review enterprise risk assessment	95%	77%	70%	85%
Approve risk policies	86%	80%	57%	78%
Oversee the bank's risk management framework	73%	77%	65%	72%
Compliance with the risk management program's policies and procedures	81%	70%	43%	71%
Oversee risk dashboard reporting	84%	57%	39%	69%
Establish risk appetite	81%	43%	61%	66%
Review the bank's cybersecurity plan	70%	55%	65%	64%
Review stress testing results	65%	66%	57%	62%
Review strategic plan and risk mitigation strategies	64%	43%	61%	57%
Review compensation risk	41%	25%	48%	36%
Other	4%	5%	-	5%
Unsure	1%	5%	4%	3%

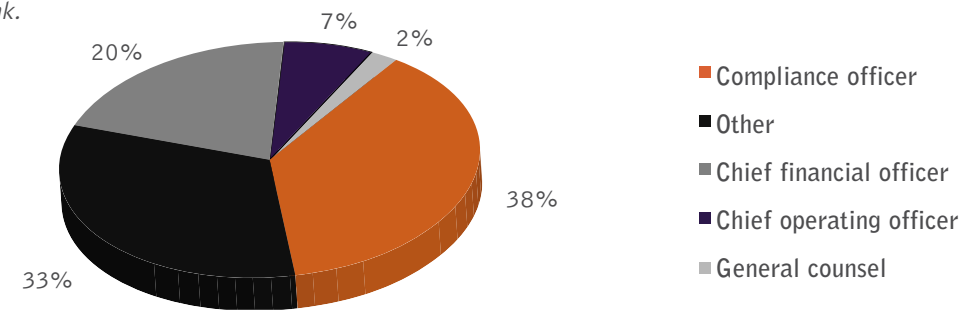
5. Does your bank have a chief risk officer or someone who has been officially designated with responsibility for overseeing the bank's risk management program?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes, and the CRO is exclusively focused on risk management	94%	81%	44%	15%	49%
Yes, but that officer is also focused on other areas of the bank	6%	15%	43%	55%	37%
No	-	4%	13%	30%	14%

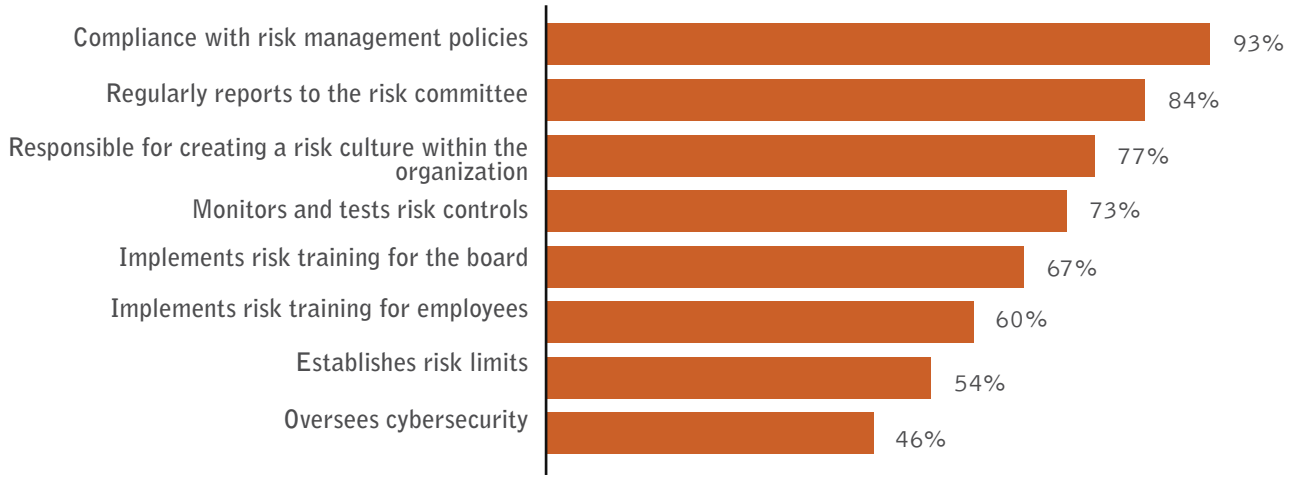
6. Who serves as the chief risk officer at your institution?

Questions only asked of respondents who indicated that the bank has a chief risk officer who is focused on other areas of the bank.



7. What are the duties of the risk officer?

Respondents were asked to select all that apply. Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.

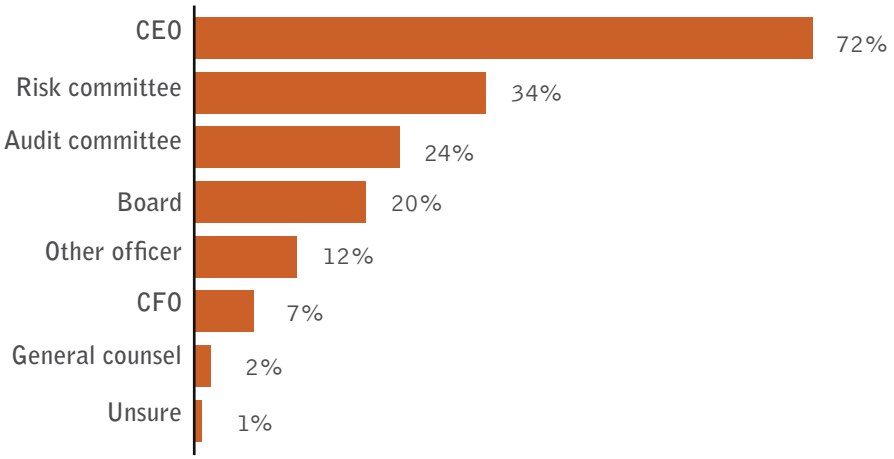


Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Compliance with risk management policies	94%	96%	91%	92%	93%
Regularly reports to the risk committee	94%	96%	86%	62%	84%
Responsible for creating a risk culture within the organization	89%	87%	73%	67%	77%
Monitors and tests risk controls	67%	65%	77%	75%	73%
Implements risk training for the board	83%	70%	64%	58%	67%
Implements risk training for employees	78%	48%	61%	54%	60%
Establishes risk limits	72%	65%	45%	50%	54%
Oversees cybersecurity	22%	52%	52%	46%	46%

The chief risk officer...	Is exclusively focused on risk management	Is also focused on other areas of the bank	Total
Compliance with risk management policies	94%	90%	93%
Regularly reports to the risk committee	90%	76%	84%
Responsible for creating a risk culture within the organization	84%	67%	77%
Monitors and tests risk controls	73%	73%	73%
Implements risk training for the board	66%	69%	67%
Implements risk training for employees	60%	59%	60%
Establishes risk limits	63%	41%	54%
Oversees cybersecurity	44%	49%	46%

8. To whom does the chief risk officer report?

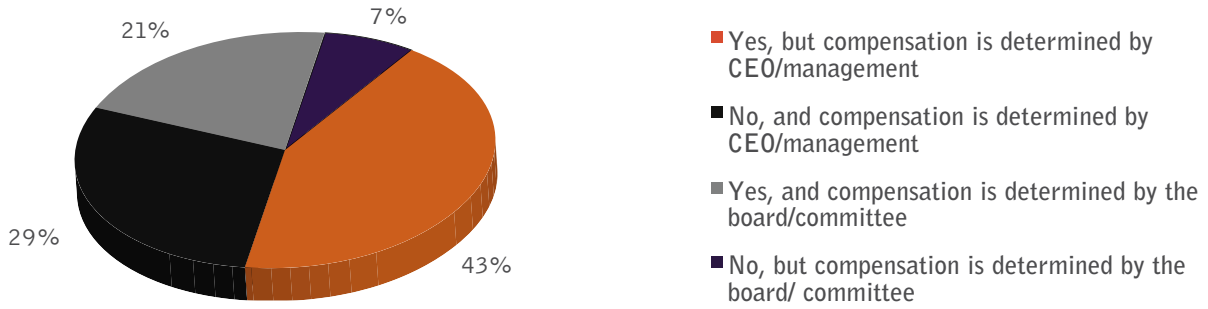
Respondents were asked to select all that apply. Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
CEO	72%	87%	62%	80%	72%
Risk committee	56%	57%	27%	12%	34%
Audit committee	-	13%	32%	32%	24%
Board	11%	22%	21%	24%	20%
Other officer	28%	4%	9%	16%	12%
CFO	-	-	14%	4%	7%
General counsel	6%	-	2%	4%	2%
Unsure	-	-	2%	-	1%

9. Is the chief risk officer's performance reviewed by the board or a board committee?

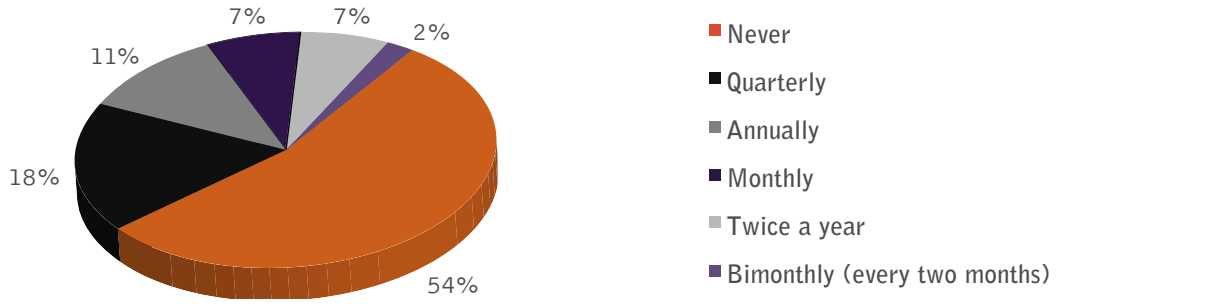
Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes, but compensation is determined by CEO/management	59%	43%	43%	32%	43%
No, and compensation is determined by CEO/management	6%	30%	38%	24%	29%
Yes, and compensation is determined by board/committee	35%	22%	14%	28%	21%
No, but compensation is determined by board/committee	-	4%	5%	16%	7%

10. How often does the chief risk officer meet in private, without management, with the board?

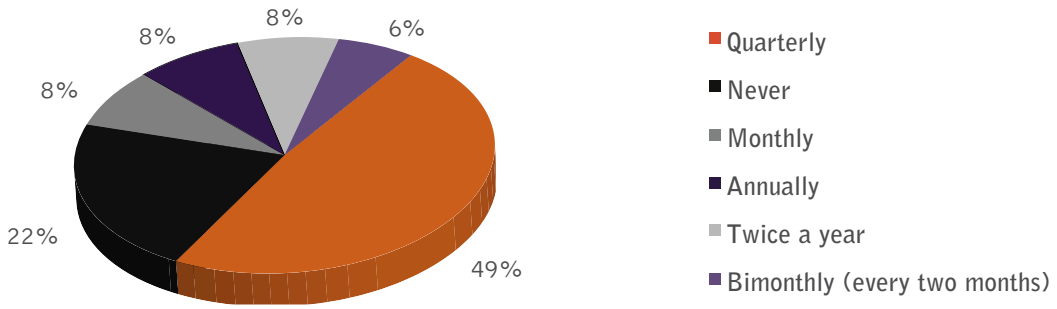
Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Never	56%	57%	50%	60%	54%
Quarterly	28%	22%	16%	12%	18%
Annually	-	13%	12%	16%	11%
Monthly	6%	4%	9%	8%	7%
Twice a year	6%	4%	9%	4%	7%
Bimonthly (every two months)	6%	-	4%	-	2%

11. How often does the chief risk officer meet in private, without management, with the committee that governs risk?

Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.

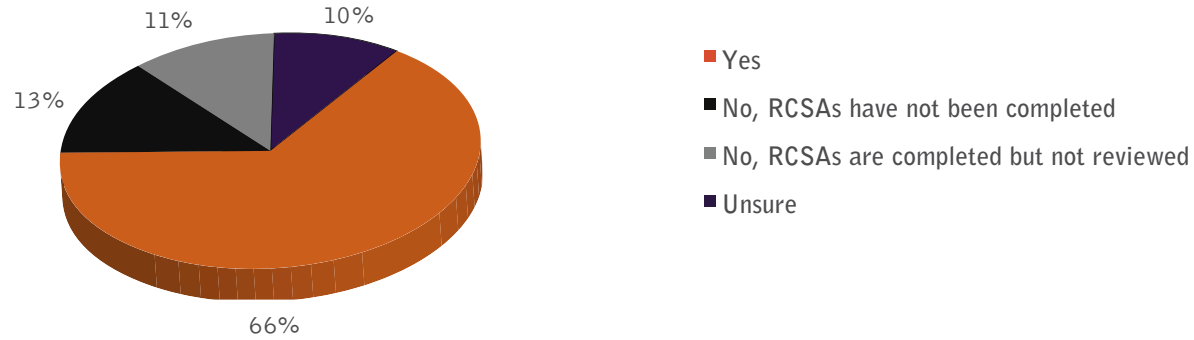


Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Quarterly	61%	59%	49%	29%	49%
Never	22%	5%	22%	38%	22%
Monthly	6%	9%	9%	8%	8%
Annually	-	14%	5%	12%	8%
Twice a year	6%	5%	7%	12%	8%
Bimonthly (every two months)	6%	9%	7%	-	6%

Bank Asset Size	Separate risk committee	Audit committee	Entire board	Total
Quarterly	58%	45%	36%	49%
Never	12%	27%	43%	22%
Monthly	9%	6%	7%	8%
Annually	5%	12%	7%	8%
Twice a year	8%	6%	7%	8%
Bimonthly (every two months)	9%	3%	-	6%

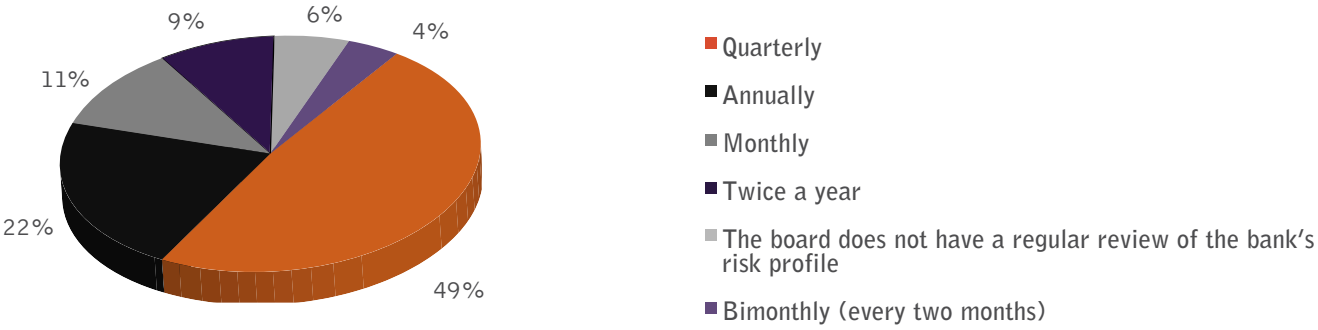
12. Are risk control self-assessments (RCSAs) completed by the chief risk officer and reviewed with the board or board committee?

Question only asked of respondents who indicated that the bank has a chief risk officer or other officer designated with overseeing risk management.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes	78%	65%	59%	72%	66%
No, RCSAs have not been completed	-	17%	20%	4%	13%
No, RCSAs are completed but not reviewed	17%	17%	5%	16%	11%
Unsure	6%	-	16%	8%	10%

13. How often does the board review the bank's risk profile and related metrics with senior management?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Quarterly	72%	68%	47%	26%	49%
Annually	17%	14%	22%	29%	22%
Monthly	-	-	10%	26%	11%
Twice a year	6%	14%	10%	6%	9%
The board does not have a regular review of the bank's risk profile	-	-	5%	14%	6%
Bimonthly (every two months)	6%	5%	5%	-	4%

RISK CULTURE & INFRASTRUCTURE

14. Looking at the overall organization, what elements are incorporated into the bank's culture to support risk management?

Respondents were asked to select all that apply.

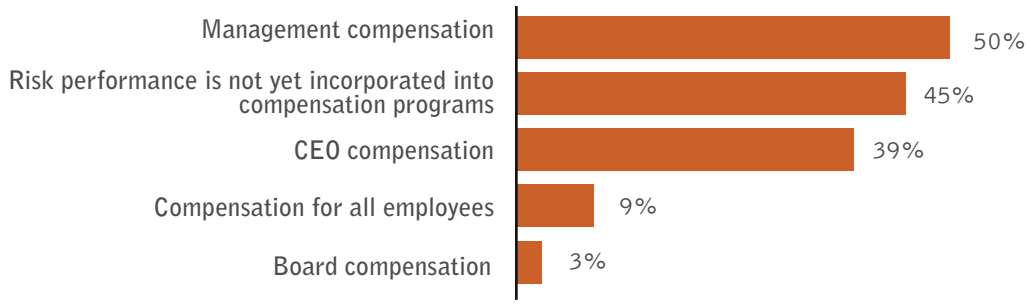
Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Defined responsibility for risk management among management and employees	83%	77%	68%	80%	75%
Regular board training on risk issues	67%	77%	59%	57%	63%
Business lines own risk and participate fully in the bank's risk management program	72%	73%	66%	37%	60%
All employees trained on risk	67%	45%	58%	60%	57%
Risk appetite statement/risk limits communicated to all employees	67%	45%	41%	26%	41%
Compensation linked to risk management performance	50%	45%	32%	26%	35%
Chairman and/or risk committee chair regularly meet with line management	72%	27%	27%	23%	32%
None of the above	-	-	3%	3%	2%
Other	-	-	2%	-	1%

Which board committee governs risk?	Separate risk committee	Audit committee	Entire board	Total
Defined responsibility for risk management among management and employees	79%	76%	52%	75%
Regular board training on risk issues	66%	65%	57%	63%
Business lines own risk and participate fully in the bank's risk management program	67%	43%	62%	60%
All employees trained on risk	51%	70%	48%	57%
Risk appetite statement/risk limits communicated to all employees	51%	22%	29%	41%
Compensation linked to risk management performance	40%	41%	5%	35%
Chairman and/or risk committee chair regularly meet with line management	39%	22%	24%	32%
None of the above	1%	-	10%	2%
Other	1%	-	-	1%

The chief risk officer...	Is exclusively focused on risk management	Is also focused on other areas of the bank	Bank doesn't have a CRO	Total
Defined responsibility for risk management among management and employees	77%	75%	63%	75%
Regular board training on risk issues	62%	60%	68%	63%
Business lines own risk and participate fully in the bank's risk management program	67%	56%	53%	60%
All employees trained on risk	59%	58%	53%	57%
Risk appetite statement/risk limits communicated to all employees	45%	42%	26%	41%
Compensation linked to risk management performance	44%	31%	16%	35%
Chairman and/or risk committee chair regularly meet with line management	41%	25%	21%	32%
None of the above	3%	2%	-	2%
Other	2%	-	-	1%

15. 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.

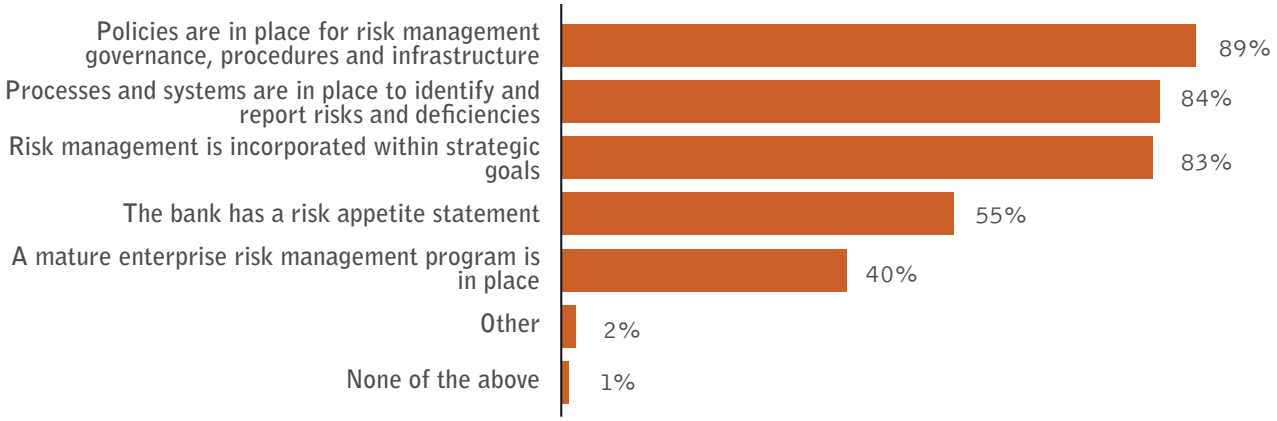


Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Management compensation	71%	62%	49%	34%	50%
Risk performance is not yet incorporated into compensation programs	29%	33%	46%	57%	45%
CEO compensation	59%	48%	35%	31%	39%
Compensation for all employees	29%	10%	7%	3%	9%
Board compensation	-	10%	4%	-	3%

Which board committee governs risk?	Separate risk committee	Audit committee	Entire board	Total
Management compensation	54%	43%	33%	50%
Risk performance is not yet incorporated into compensation programs	43%	49%	57%	45%
CEO compensation	43%	34%	24%	39%
Compensation for all employees	14%	6%	-	9%
Board compensation	2%	3%	10%	3%

16. Looking at the overall organization, what elements are incorporated into the bank's infrastructure to support risk management?

Respondents were asked to select all that apply.

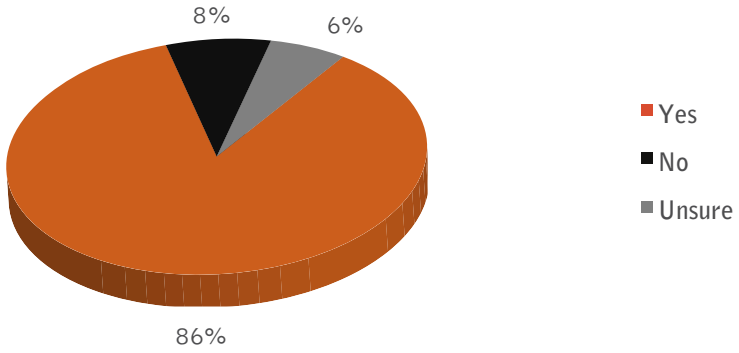


Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Policies are in place for risk management governance, procedures and infrastructure	100%	95%	86%	83%	89%
Processes and systems are in place to identify and report risks and deficiencies	89%	82%	88%	74%	84%
Risk management is incorporated within strategic goals	89%	86%	83%	77%	83%
The bank has a risk appetite statement	89%	73%	59%	20%	55%
A mature enterprise risk management program is in place	67%	41%	32%	37%	40%
Other	-	-	5%	-	2%
None of the above	-	-	-	3%	1%

Which board committee governs risk?	Separate risk committee	Audit committee	Entire board	Total
Policies are in place for risk management governance, procedures and infrastructure	94%	89%	76%	89%
Processes and systems are in place to identify and report risks and deficiencies	90%	76%	76%	84%
Risk management is incorporated within strategic goals	87%	78%	76%	83%
The bank has a risk appetite statement	72%	43%	14%	55%
A mature enterprise risk management program is in place	43%	38%	29%	40%
Other	1%	5%	-	2%
None of the above	-	-	5%	1%

The chief risk officer ...	Is exclusively focused on risk management	Is also focused on other areas of the bank	Bank doesn't have a CRO	Total
Policies are in place for risk management governance, procedures and infrastructure	94%	90%	68%	89%
Processes and systems are in place to identify and report risks and deficiencies	83%	83%	84%	84%
Risk management is incorporated within strategic goals	89%	77%	79%	83%
The bank has a risk appetite statement	70%	50%	21%	55%
A mature enterprise risk management program is in place	45%	35%	32%	40%
Other	3%	2%	-	2%
None of the above	-	2%	-	1%

17. Do you believe that your institution has the appropriate culture and infrastructure in place to manage risk?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes	89%	86%	83%	89%	86%
No	-	10%	8%	11%	8%
Unsure	11%	5%	8%	-	6%

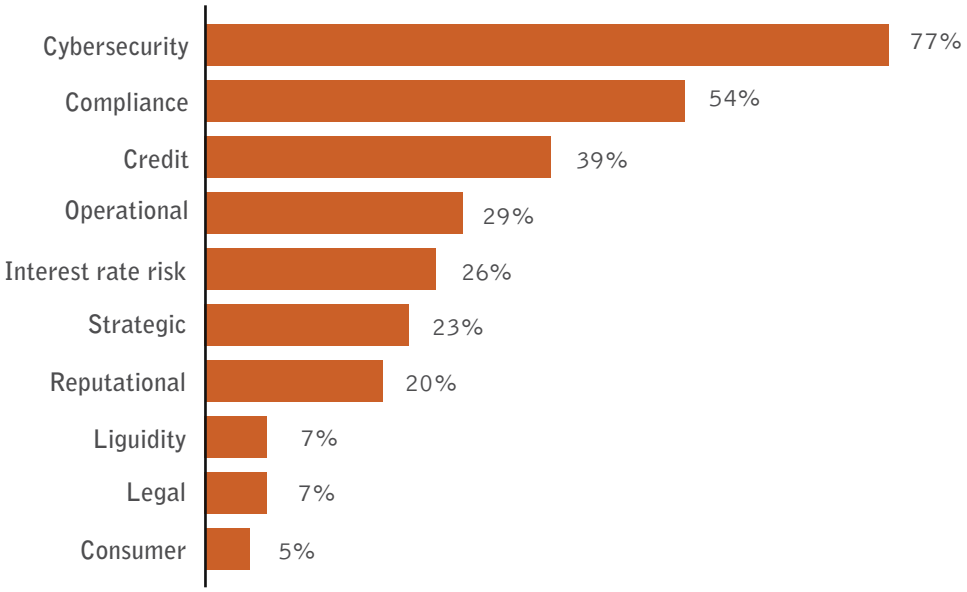
18. What are your bank's three biggest risk management challenges?

Respondents were asked to select no more than three.

Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Preparing for cyberattacks	39%	67%	59%	52%	55%
Keeping up with regulatory expectations of risk management practices	83%	43%	53%	42%	53%
Maintaining the technology and data infrastructure to support risk decision-making	61%	57%	38%	36%	44%
Fully implementing enterprise risk management (ERM)	44%	24%	43%	30%	37%
Creating a culture that supports bank-wide risk communication and assessment	17%	38%	31%	27%	29%
Clearly defining the institution's risk tolerances	6%	24%	29%	39%	28%
Having the in-house risk expertise	6%	10%	16%	21%	15%
Making a financial commitment to technology, consulting or training	11%	10%	10%	24%	14%

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

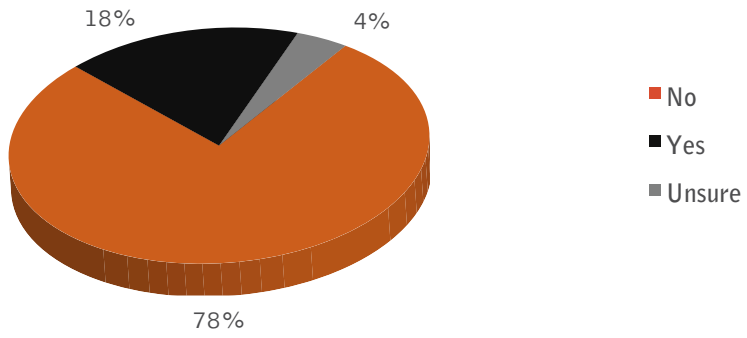
Respondents were asked to select no more than three.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Cybersecurity	67%	81%	79%	77%	77%
Compliance	61%	52%	57%	46%	54%
Credit	17%	43%	47%	37%	39%
Operational	33%	33%	31%	20%	29%
Interest rate risk	33%	5%	31%	26%	26%
Strategic	28%	38%	12%	29%	23%
Reputational	17%	14%	17%	31%	20%
Liquidity	6%	14%	5%	6%	7%
Legal	11%	5%	7%	6%	7%
Consumer	22%	-	3%	3%	5%

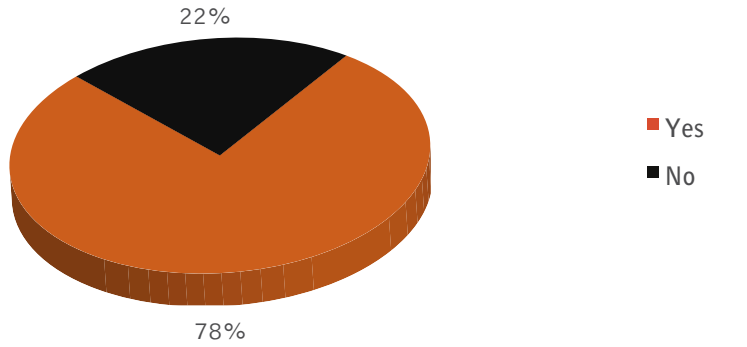
CYBERSECURITY

20. Has your bank experienced a data breach?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
No	71%	81%	78%	80%	78%
Yes	24%	19%	19%	14%	18%
Unsure	6%	-	3%	6%	4%

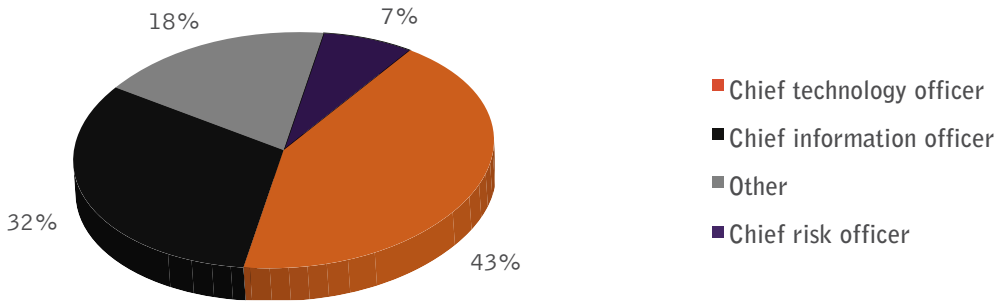
21. Does your bank have a full-time chief information security officer?



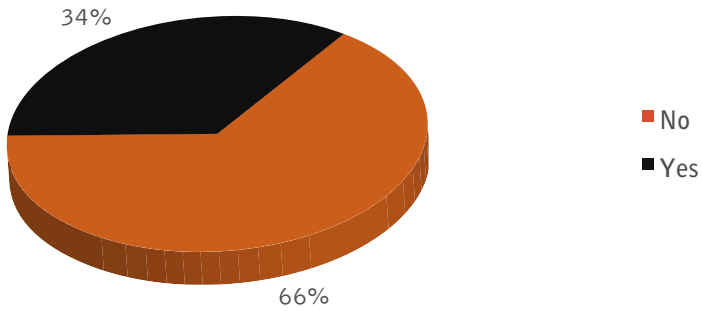
Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes	94%	95%	76%	63%	78%
No	6%	5%	24%	37%	22%

22. Who handles information security/cybersecurity at your bank?

Question only asked of respondents who indicated their bank does not have a full-time chief information security officer.



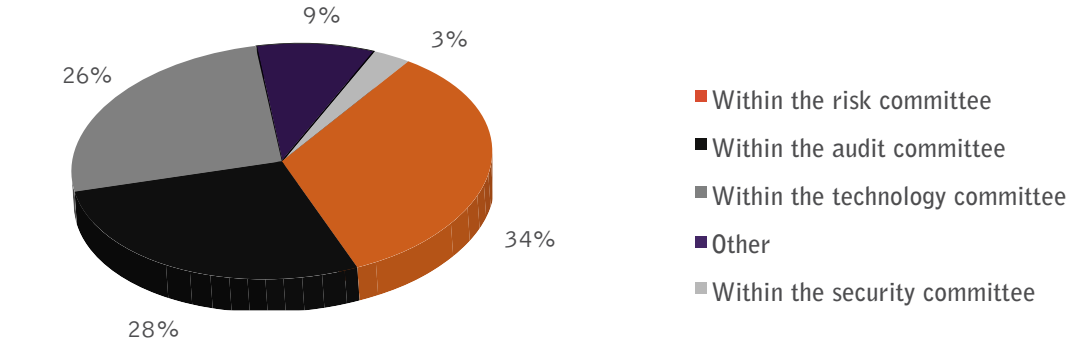
23. Does your board review cybersecurity at every board meeting?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
No	65%	57%	69%	69%	66%
Yes	35%	43%	31%	31%	34%

Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
No	62%	83%	66%
Yes	38%	17%	34%

24. How does the board primarily handle cybersecurity governance?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Within the risk committee	61%	71%	23%	14%	34%
Within the audit committee	6%	19%	39%	29%	28%
Within the technology committee	28%	-	30%	34%	26%
Other	6%	5%	7%	17%	9%
Within the security committee	-	5%	2%	6%	3%

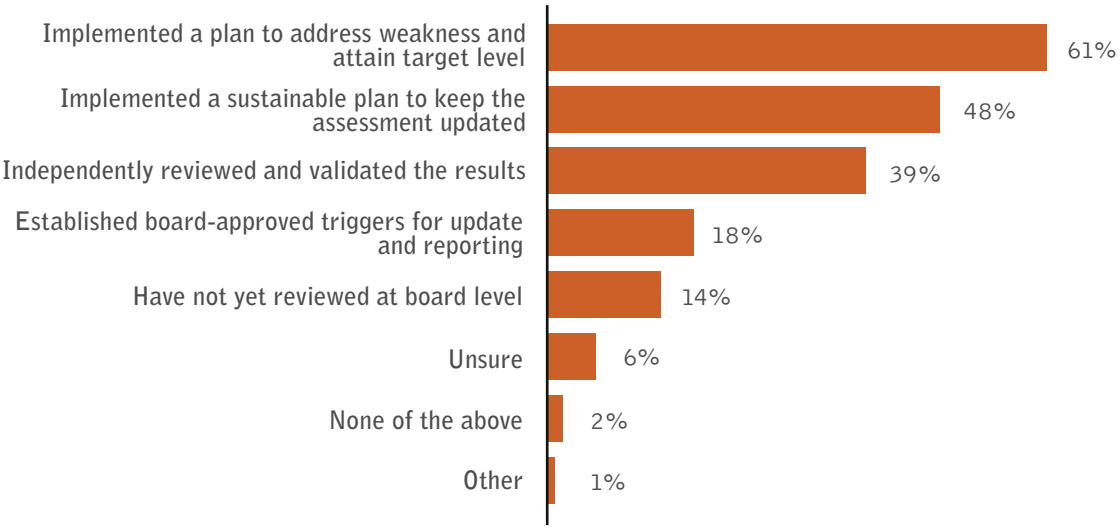
25. Has your bank used the new FFIEC Cybersecurity Assessment Tool and completed an assessment?

Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Yes, our bank has used the tool and completed an assessment	53%	71%	68%	50%	62%
Our bank has used the tool, but not yet completed an assessment	18%	10%	19%	12%	16%
I don't know or understand what the cybersecurity assessment tool is	24%	14%	4%	15%	11%
No, but our bank plans to use the tool and complete an assessment soon	6%	5%	5%	15%	8%
No, our bank has not used the tool or completed an assessment	-	-	4%	9%	4%

Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Yes, our bank has used the tool and completed an assessment	66%	45%	62%
Our bank has used the tool, but not yet completed an assessment	14%	21%	16%
I don't know or understand what the cybersecurity assessment tool is	11%	11%	11%
No, but our bank plans to use the tool and complete an assessment soon	7%	11%	8%
No, our bank has not used the tool or completed an assessment	2%	11%	4%

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

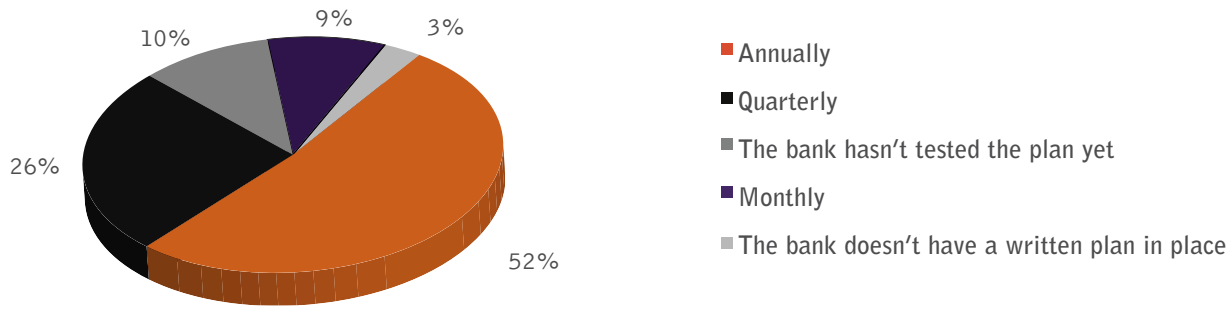
Respondents were asked to select all that apply. Question only asked of respondents who indicated that the bank has used the FFIEC cybersecurity tool and completed an assessment.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Implemented a plan to address weaknesses and attain target level	78%	67%	64%	41%	61%
Implemented a sustainable plan to keep the assessment updated	67%	27%	46%	59%	48%
Independently reviewed and validated the results	33%	47%	36%	41%	39%
Established board-approved triggers for update and reporting	22%	20%	15%	18%	18%
Have not yet reviewed at board level	-	13%	18%	12%	14%
Unsure	11%	7%	5%	6%	6%
None of the above	-	-	5%	-	2%
Other	-	-	-	6%	1%

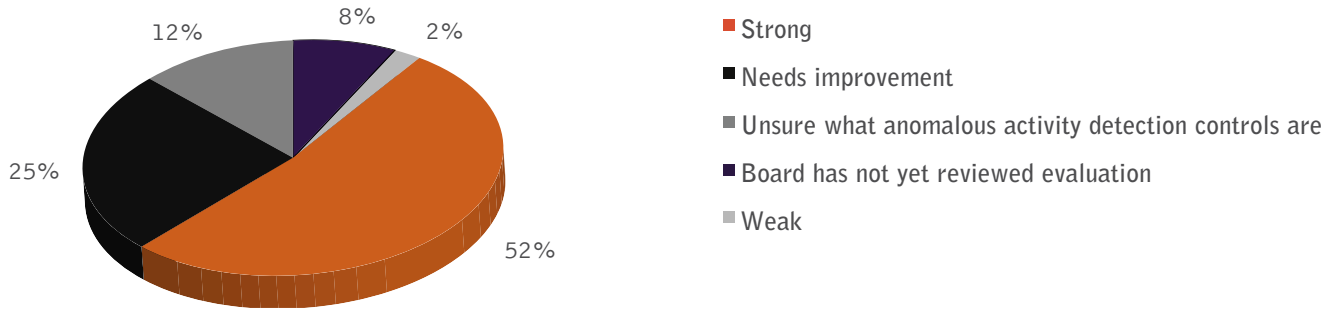
Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Implemented a plan to address weaknesses and attain target level	66%	38%	61%
Implemented a sustainable plan to keep the assessment updated	43%	69%	48%
Independently reviewed and validated the results	40%	31%	39%
Established board-approved triggers for update and reporting	19%	8%	18%
Have not yet reviewed at board level	15%	8%	14%
Unsure	7%	-	6%
None of the above	1%	8%	2%
Other	1%	-	1%

27. How often does your bank test its written cyber-incident management and response plan?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Annually	50%	61%	52%	48%	52%
Quarterly	25%	22%	23%	32%	26%
The bank hasn't tested the plan yet	-	11%	15%	6%	10%
Monthly	19%	6%	8%	6%	9%
The bank doesn't have a written plan in place	6%	-	2%	6%	3%

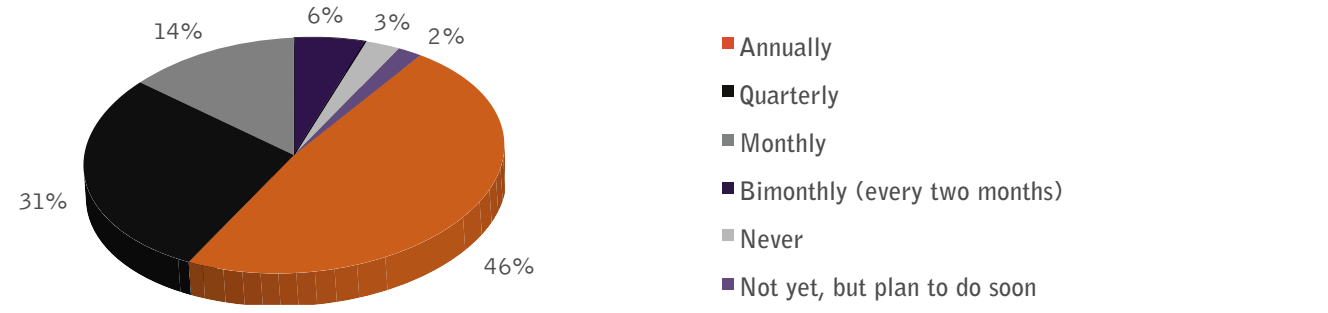
28. How would you evaluate your bank's anomalous activity detection controls?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Strong	59%	44%	39%	73%	52%
Needs improvement	24%	28%	37%	6%	25%
Unsure what anomalous activity detection controls are	6%	22%	13%	9%	12%
Board has not yet reviewed evaluation	12%	-	7%	12%	8%
Weak	-	6%	4%	-	2%

Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Strong	55%	40%	52%
Needs improvement	25%	28%	25%
Unsure what anomalous activity detection controls are	13%	8%	12%
Board has not yet reviewed evaluation	4%	24%	8%
Weak	3%	-	2%

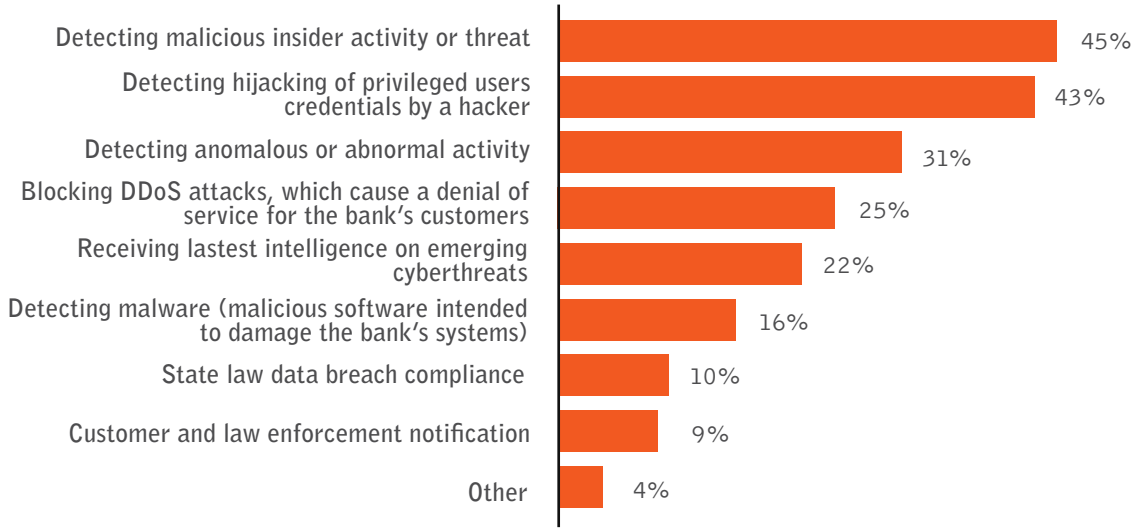
29. How often do you test bank employees' susceptibility to phishing and social engineering attacks and schemes?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Annually	18%	47%	52%	50%	46%
Quarterly	41%	35%	25%	31%	31%
Monthly	35%	6%	10%	12%	14%
Bimonthly (every two months)	6%	12%	8%	-	6%
Never	-	-	4%	3%	3%
Not yet, but plan to do soon	-	-	2%	3%	2%

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

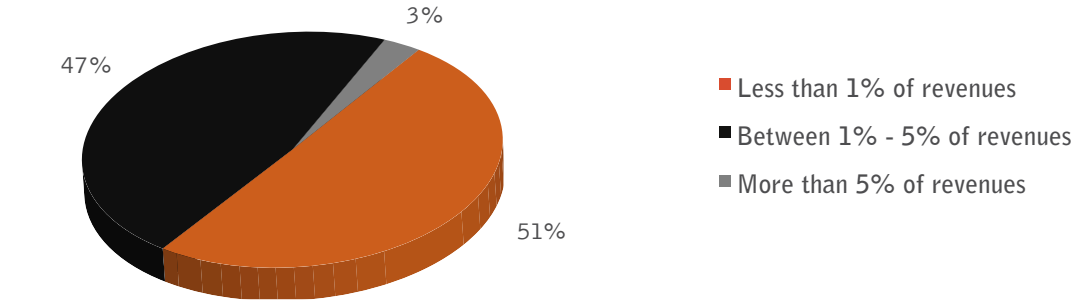
Respondents were asked to select all that apply.



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Detecting malicious insider activity or threat	38%	41%	52%	39%	45%
Detecting hijacking of privileged users credentials by a hacker	46%	41%	38%	50%	43%
Detecting anomalous or abnormal activity	23%	47%	29%	29%	31%
Blocking DDoS attacks, which cause a denial of service for the bank's customers	38%	12%	23%	32%	25%
Receiving latest intelligence on emerging cyberthreats	23%	24%	21%	21%	22%
Detecting malware (malicious software intended to damage the bank's systems)	15%	12%	13%	25%	16%
State law data breach compliance	15%	6%	12%	7%	10%
Customer and law enforcement notification	15%	-	12%	7%	9%
Other	15%	6%	2%	-	4%

Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Detecting malicious insider activity or threat	42%	59%	45%
Detecting hijacking of privileged users credentials by a hacker	40%	55%	43%
Detecting anomalous or abnormal activity	30%	36%	31%
Blocking DDoS attacks, which cause a denial of service for the bank's customers	28%	14%	25%
Receiving latest intelligence on emerging cyberthreats	23%	18%	22%
Detecting malware (malicious software intended to damage the bank's systems)	17%	14%	16%
State law data breach compliance	11%	5%	10%
Customer and law enforcement notification	9%	9%	9%
Other	5%	-	4%

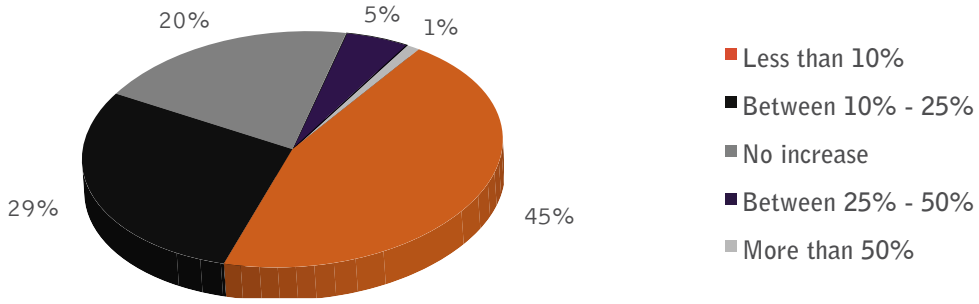
31. How large was your bank's cybersecurity budget for fiscal year 2015?



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Less than 1% of revenues	53%	44%	50%	55%	51%
Between 1% - 5% of revenues	41%	56%	48%	41%	47%
More than 5% of revenues	6%	-	2%	3%	3%

Does the bank have a full-time CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Less than 1% of revenues	48%	61%	51%
Between 1% - 5% of revenues	48%	39%	47%
More than 5% of revenues	3%	-	3%

32. How much has your bank's cybersecurity budget increased for FY 2016?



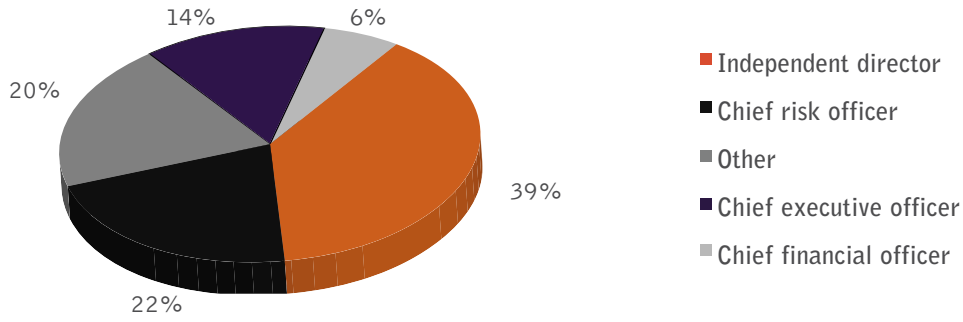
Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Less than 10%	36%	22%	57%	41%	45%
Between 10% - 25%	43%	61%	17%	24%	29%
No increase	7%	17%	19%	31%	20%
Between 25% - 50%	14%	-	6%	3%	5%
More than 50%	-	-	2%	-	1%

Does the bank have a CISO?	Bank has a CISO	Bank doesn't have a CISO	Total
Less than 10%	45%	43%	45%
Between 10% - 25%	30%	26%	29%
No increase	18%	30%	20%
Between 25% - 50%	7%	-	5%
More than 50%	1%	-	1%

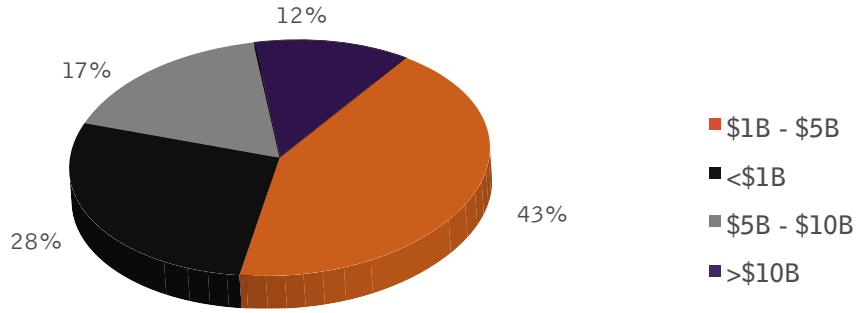
ABOUT THE SURVEY

Bank Director's 2016 Risk Practices Survey, sponsored by FIS, surveyed 161 chief risk officers, senior executives and independent directors of U.S. banks with more than $500 million in assets to examine risk management practices and governance trends, as well as how banks govern and manage cybersecurity risk. The online survey was conducted in January 2016. Forty-four percent of participants serve as an independent director or chairmen at their bank. Twenty-two percent are chief risk officers, and 14 percent serve as the bank's CEO. A majority of respondents, 43 percent, represent institutions with between $1 billion and $5 billion in assets. Twenty-nine percent represent banks above $5 billion in assets, and 28 percent institutions below $1 billion.

Title Breakdown



Bank Asset Size



Bank Asset Size	>$10B	$5B - $10B	$1B - $5B	<$1B	Total
Median return on equity (ROE)	9.2	8.9	8.1	6.0	8.2
Median return on assets (ROA)	1.0	1.0	1.0	0.7	1.0