2025

CYBER SECURITY REPORT

FOR THE FINANCIAL INSTITUTION INDUSTRY

Tandem®

Contents

About the Report

This report includes the results of a survey of cybersecurity professionals working in the financial institution industry in the United States. The survey resulted in 310 responses which led to several informative observations about how community financial institutions manage and can improve their cybersecurity posture.

Purpose

The purpose of this report is to identify how financial institutions are navigating cybersecurity, including emerging trends, challenges, and best practices. Specifically, this report explores:

- Oversight of cybersecurity by boards, senior management, and examiners
- Resource allocation, including staffing levels and budget priorities
- Training, awareness, and building a strong security culture
- Operational risk management, such as vendor management, incident response, and business continuity
- Emerging technologies and their impact on cybersecurity strategy

Timeframe

This survey was conducted between June 2, 2025 and July 31, 2025.

Participants

All 310 survey participants work for a financial institution based in the United States.

Author

The survey was conducted by Tandem, LLC. For more information about Tandem, visit Tandem.App.

Method

Survey results were reviewed by a team of cybersecurity experts and analysts at Tandem. The results displayed in this report feature trends across years and correlations between questions. Only significant answer options are represented in the observations. This means percentages are rounded to the nearest whole number and not all percentage totals in this report equal 100%. To participate in future surveys, visit Tandem.App/Survey-Sign-Up.

Structure

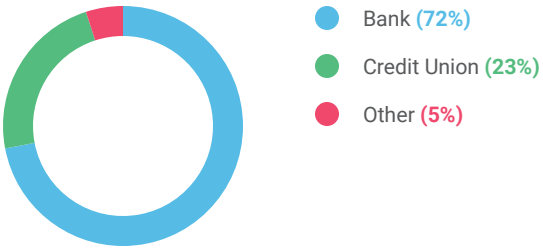
The report is structured into sections for each survey topic. Each section may feature one or more subsections to better organize and share results, including:

- Observations: An overview of findings from the survey.
- Diving Further: Deeper insights to highlight trends, cross-reference responses, or compare with prior years.
- Commentary: Additional perspectives on the subject, including summaries, opinions, or recommendations.
- Culture Impact: New to this year's report, the culture impact shows how certain topics relate to an institution's top-down cybersecurity culture, as explained in the "Information Security Culture" section.

Demographics

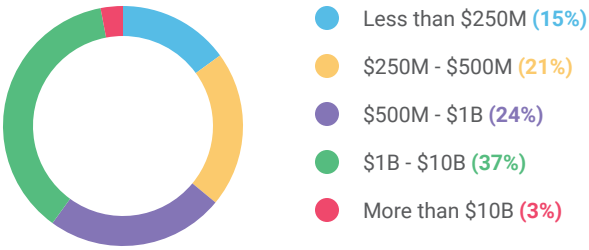
Institutions Surveyed: Types

Of those who responded, 72% work for a bank, 23% work for a credit union, and the remaining participants work for other financial institutions (e.g., mortgage companies, trust companies).



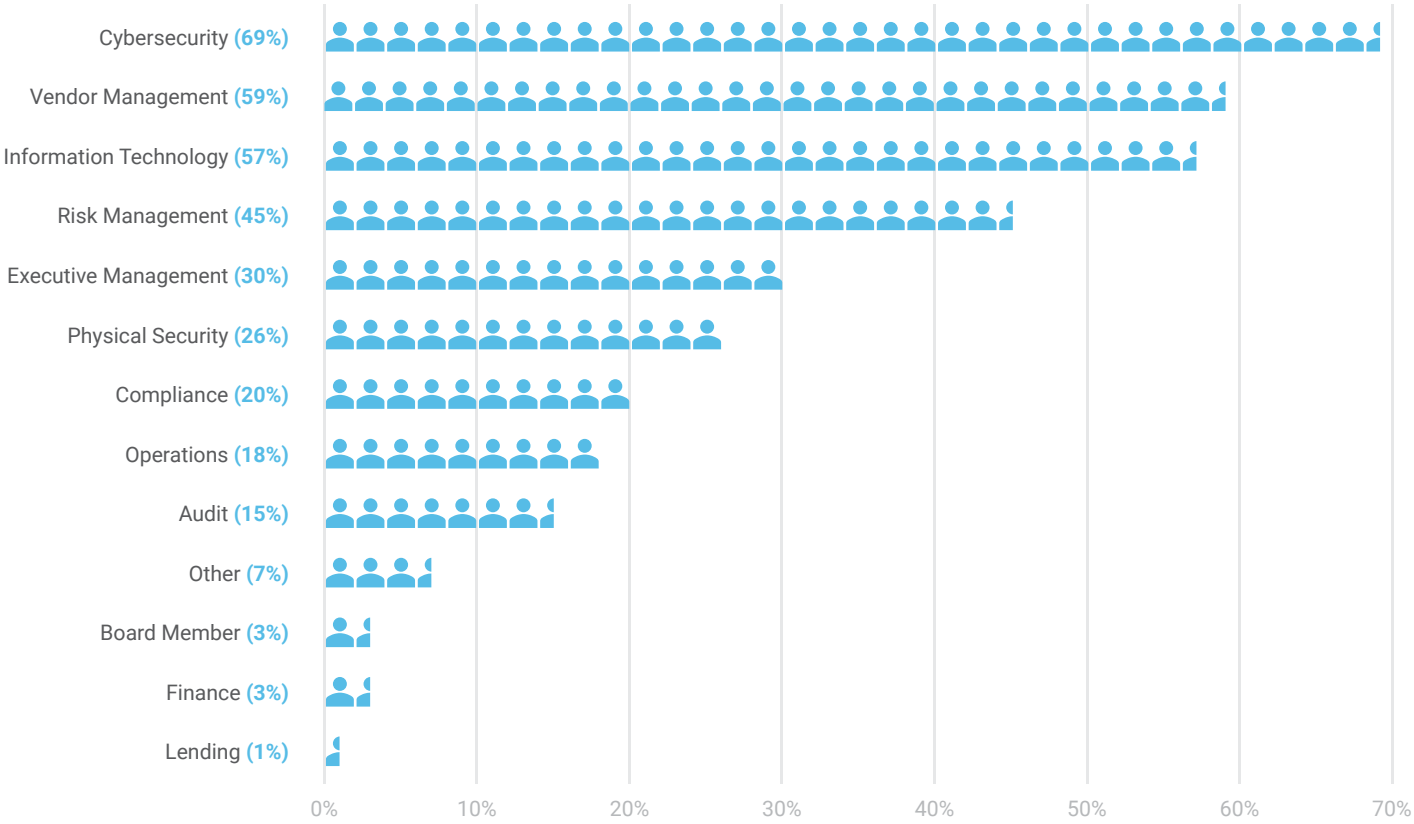
Institutions Surveyed: Assets

Survey respondents from small to medium-sized community institutions made up a majority of total respondents (60%), while 40% were from larger community institutions reporting over $1 billion in assets.



Roles & Responsibilities

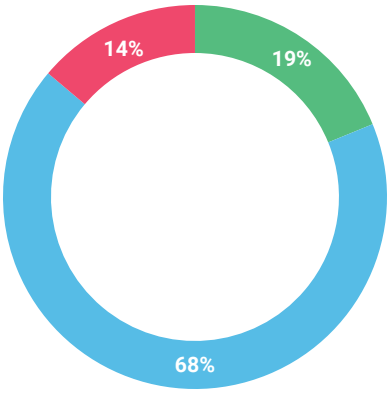
Survey participants worked primarily within cybersecurity, information technology, and vendor management roles. Participants were asked to select all that applied.



Cybersecurity Culture

We asked respondents to select the option that best represented their institution's top-down cybersecurity culture. The majority of respondents expressed while cybersecurity is important, it isn't a central driver of organizational strategy. Fourteen percent claimed cybersecurity was only done for compliance reasons or was "just a cost of doing business."

CYBERSECURITY CULTURE SET BY EXECUTIVES & OVERALL LEADERSHIP



- **Strong Culture.** Cybersecurity is deeply embedded in our culture. We integrate it into planning, budgeting, and daily operations as it is a central driver of organizational strategy. **(19%)**
- **Established Culture.** Cybersecurity is important and well-supported. We invest consistent attention and resources, though it is not a central driver of organizational strategy. **(68%)**
- **Developing Culture.** Cybersecurity is necessary for compliance. We focus on meeting examiner expectations, but it is not viewed as a competitive or strategic priority. (14%)

CULTURE IMPACT

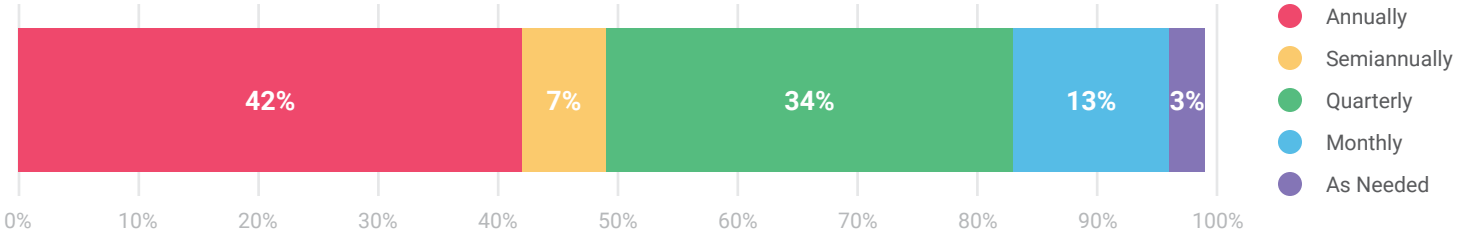
We cross analyzed this question with several other questions and created several "Culture Impact" sections throughout the report.

Board Oversight

Observation: Majority Update the Board Quarterly or Annually

Survey results show most financial institutions provide their Board of Directors with cybersecurity updates on a regular schedule, with 42% delivering a comprehensive update annually and 34% doing so quarterly. This indicates that while annual reporting remains the most common practice, a significant portion of institutions are prioritizing more frequent oversight by engaging their boards on a quarterly basis.

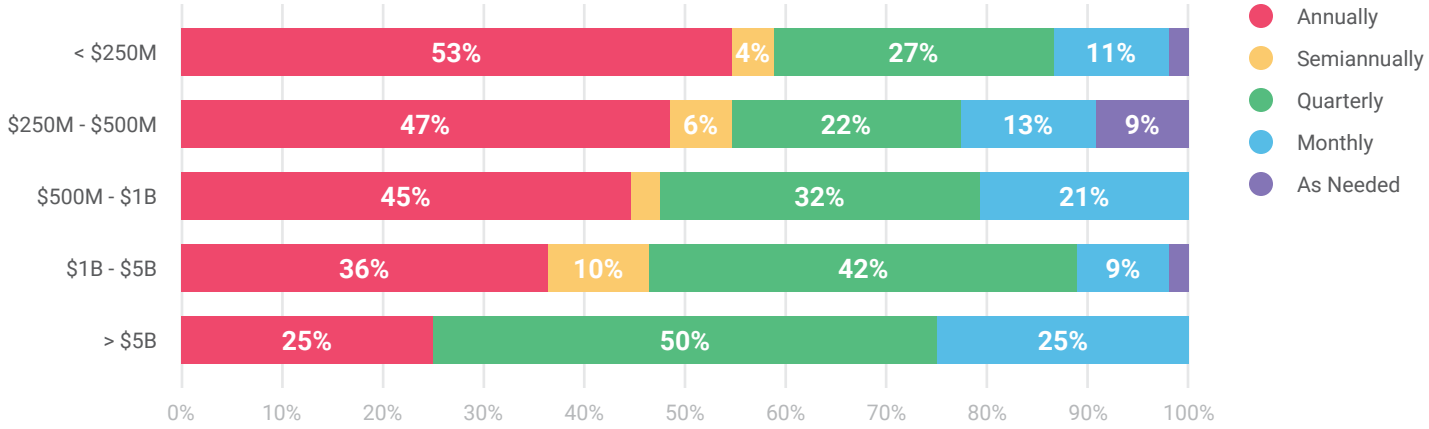
FREQUENCY OF BOARD UPDATES



Diving Further

Analyzing the data by asset size, it is interesting to see that as institutions grow in asset size, the likelihood they will report to their Board about cybersecurity also increases. For institutions under $1 billion in assets, the most likely cyber reporting frequency is annually, but for institutions over $1 billion in assets, the most likely reporting frequency is quarterly.

FREQUENCY OF BOARD UPDATES BY ASSET SIZE



Commentary

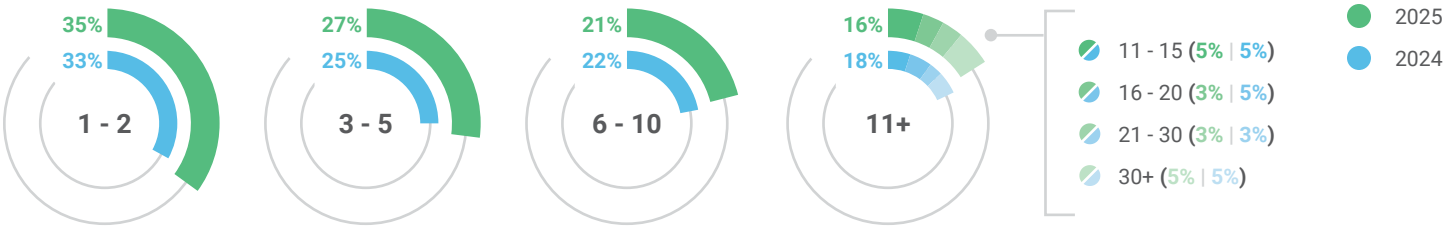
Smaller organizations may stick with annual updates because of limited resources, while larger organizations often report more often to keep up with the pace of change and regulatory expectations. If annual reporting is all you can manage, think about supplementing it with quick project updates or simple training sessions. Even small steps can go a long way in helping your Board feel prepared and confident in their oversight role.

Staffing

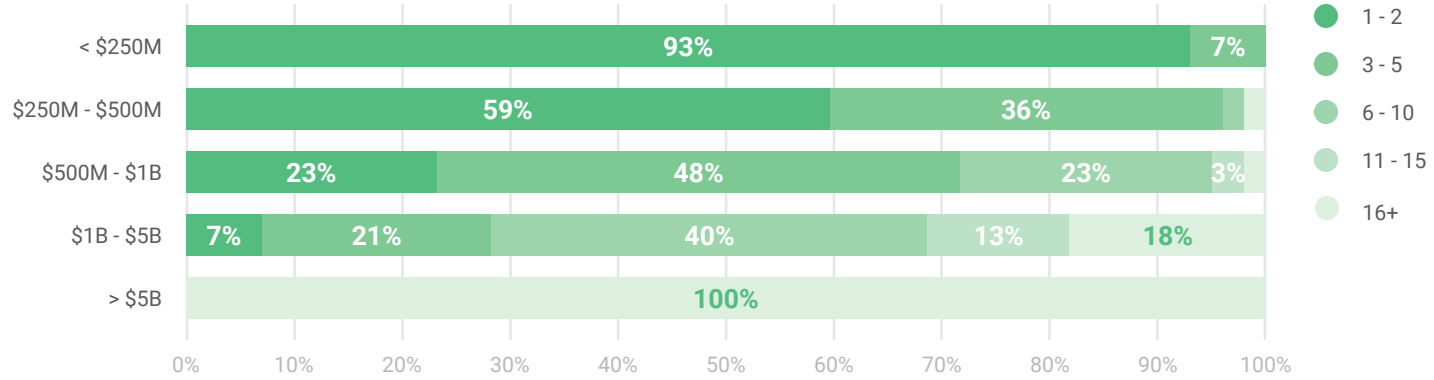
Observation: Staff Sizes Remain Unchanged in 2025

Most institutions (83%) have 10 or fewer full-time IT or information security professionals working for their institution. As might be expected, the larger the institution, the more IT and security staff are employed at the company.

NUMBER OF FULL-TIME IT AND SECURITY STAFF



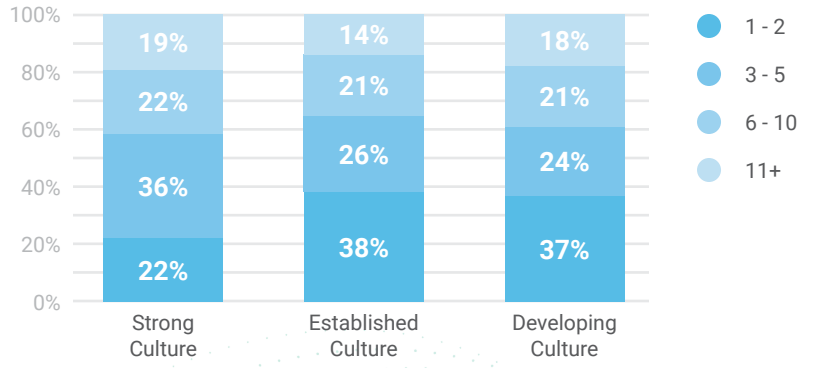
NUMBER OF FULL-TIME IT AND SECURITY STAFF BY ASSET SIZE



Culture Impact: Strong Culture Correlates with More Staff

The data shows a clear connection between organizational culture and the size of the IT team. Institutions who prioritize a strong cybersecurity culture tend to build larger teams, reflecting a deeper investment in security beyond baseline requirements. In contrast, organizations who approach cybersecurity primarily as a compliance obligation tend to operate with smaller IT teams, which may limit their ability to proactively strengthen their overall security posture. This highlights how culture not only shapes strategy but also directly influences resource allocation.

CYBERSECURITY CULTURE IMPACT ON STAFF



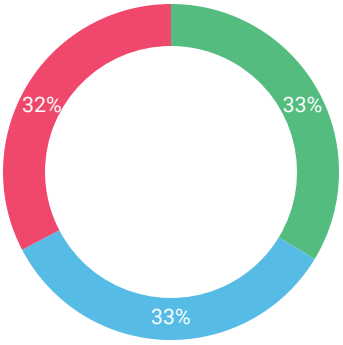
Diving Further

Digging deeper into the makeup of the IT team, the survey findings show a clear correlation of financial institution asset size and the separation of duties between information security and information technology. Of the smallest institutions, 44% report the information security and IT staff are the same person or people. Conversely, of the largest institutions, 63% report the ISO staff and IT staff are different and report to different supervisors.

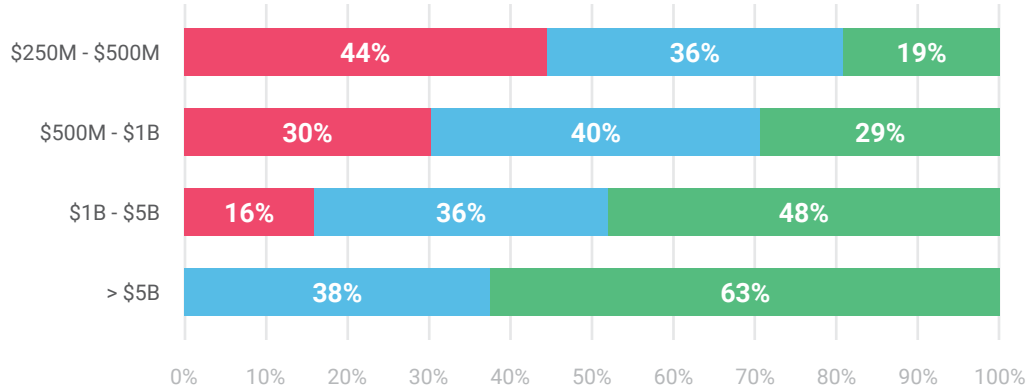
SEPARATION OF DUTIES BETWEEN IT AND SECURITY

- Information security and IT staff are the same person or people.
- Information security and IT staff are different people, both reporting to the same supervisor.
- Information security and IT staff are different people and report to different supervisors or directly to the board.

All Responses



Responses by Asset Size



Commentary

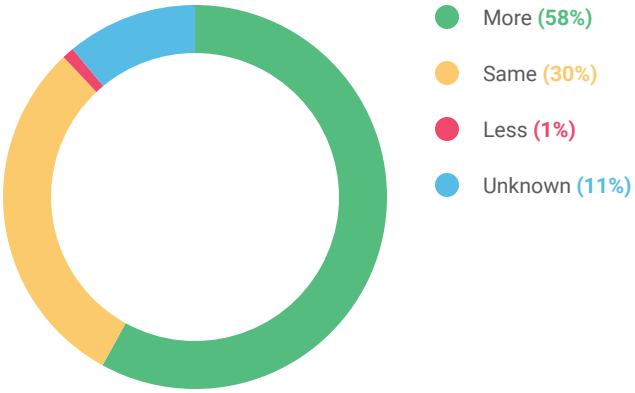
For smaller institutions, this is often a natural outcome of limited staffing and resources. In these cases, compensating controls like periodic reviews, separation of duties at the task level, board or steering committee oversight, strategic use of third-parties, or independent audits can help strengthen accountability and reduce risk without adding burden or complexity.

Budget

Observation: IT and Cyber Budgets are Increasing in 2025

Most financial institutions anticipate growth in their IT and cybersecurity budgets, with 58% expecting an increase in 2025. In contrast, 30% expect their budgets to remain the same, and only a small minority foresee a decrease. This trend reflects a continued emphasis on strengthening technology infrastructure and security measures in response to evolving threats and regulatory expectations.

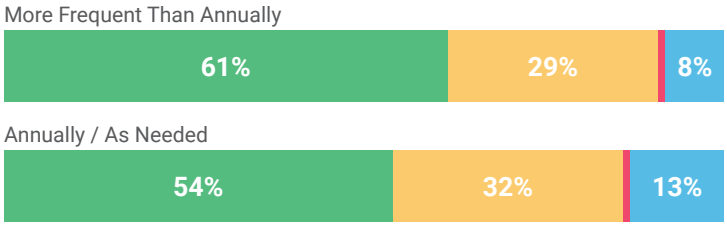
BUDGET CHANGES IN 2025



Diving Further

The data suggests regularly scheduled reports to the Board will likely lead to increased budget. Of those who report on a quarterly basis, 58% are expecting more budget in 2025 compared to 33% who only report on an as-needed basis.

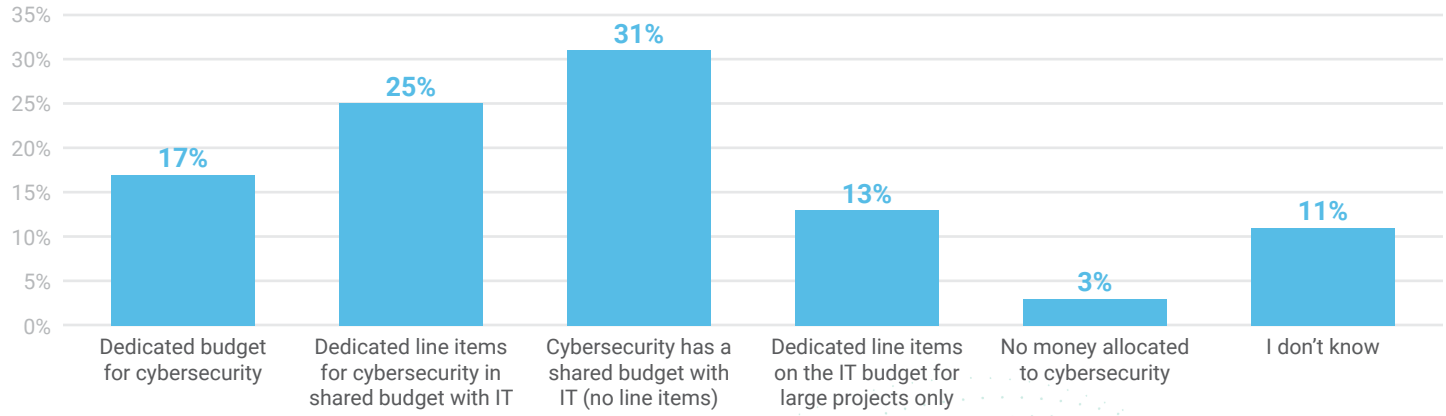
BUDGET CHANGE BY REPORT FREQUENCY



Observation: Most Cybersecurity Budgets are Shared with IT

Although some organizations maintain a dedicated cybersecurity budget, most integrate it within the IT budget. Nearly 70% report shared funding arrangements, while only 17% allocate cybersecurity as a fully separate budget.

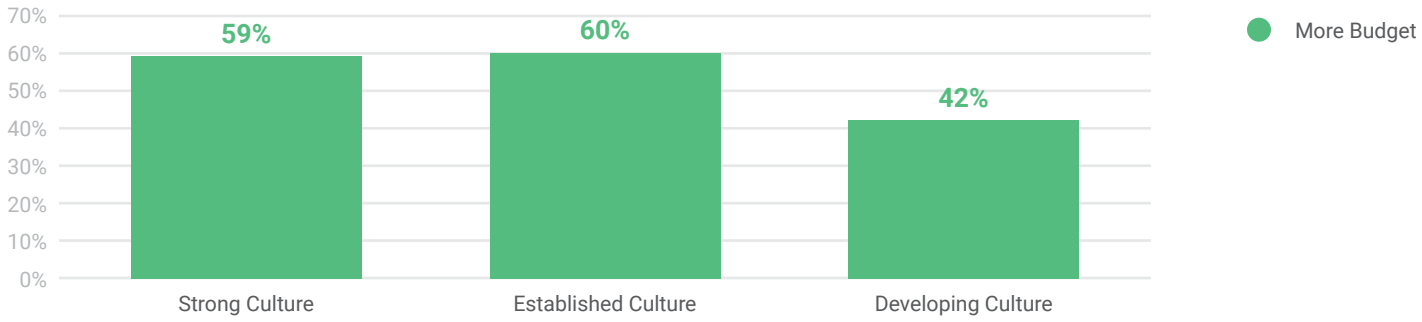
ALLOCATION OF CYBERSECURITY BUDGET



Culture Impact: Strong Culture Correlates with More Budget

The data shows a link between cybersecurity culture and budget growth. Among institutions who describe their cultures as strong, 59% report a budget increase for 2025. Similarly, 60% of institutions who say “cybersecurity is important but not a strategic driver” also report budget growth. This trend highlights when leadership treats cybersecurity as a strategic priority, investment tends to follow.

CYBERSECURITY CULTURE IMPACT ON BUDGET



Commentary

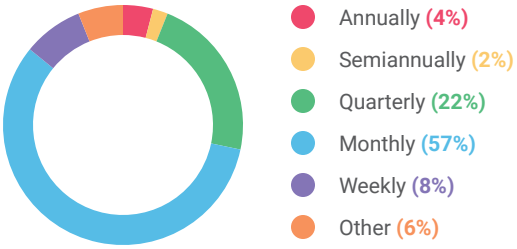
Stronger cultures bring leadership, IT, and cybersecurity onto the same page, making it easier to plan and allocate resources where they’ll make the biggest impact. On the other hand, weaker cultures often find themselves reacting, spending only when pushed by regulations or after an incident. The good news is culture can be strengthened over time. Even small steps, like increasing cross-team collaboration or giving cybersecurity leaders a stronger voice in strategic discussions, can set the stage for lasting improvements.

Training

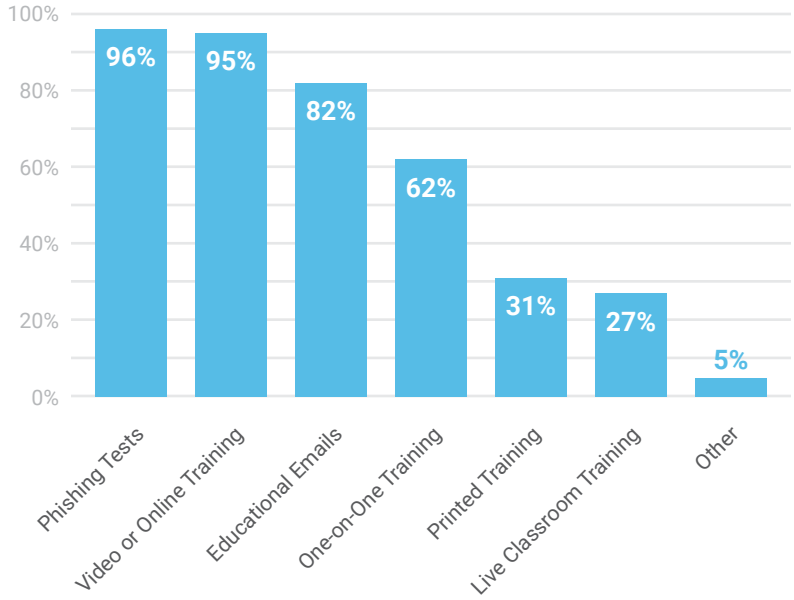
Observation: Most Perform Monthly or Quarterly Phishing Tests

Phishing tests are the most widely used form of security awareness training, with 96% of financial institutions incorporating them into their programs. Among these, 65% administer the tests monthly or more often, reflecting a strong and consistent effort to keep employees alert to social engineering tactics, which remain one of the most common and effective cybersecurity threats.

FREQUENCY OF PHISHING TESTS



TYPES OF SECURITY AWARENESS TRAINING

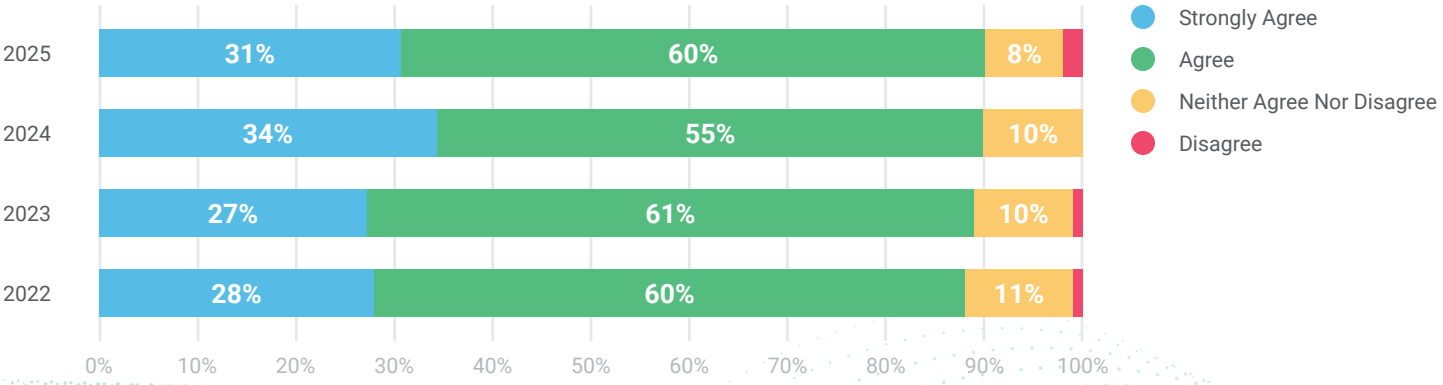


Diving Further

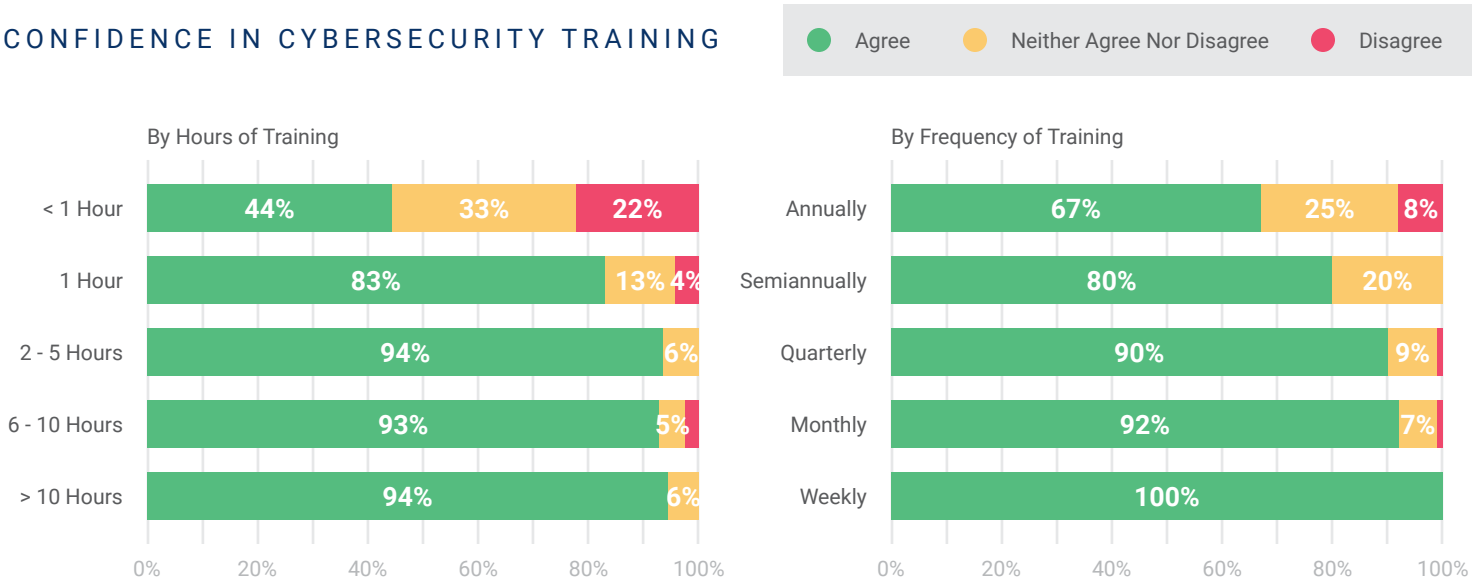
Confidence in security awareness training has stayed largely consistent over the years with 31% stating they strongly agree their cybersecurity training directly reduces the risk of an incident.

Institutions report higher confidence in their security awareness programs when they provide at least two hours of training annually and offer training sessions more than once per year. This suggests both the depth and frequency of training play a key role in building employee awareness of cybersecurity threats.

CONFIDENCE IN CYBERSECURITY TRAINING



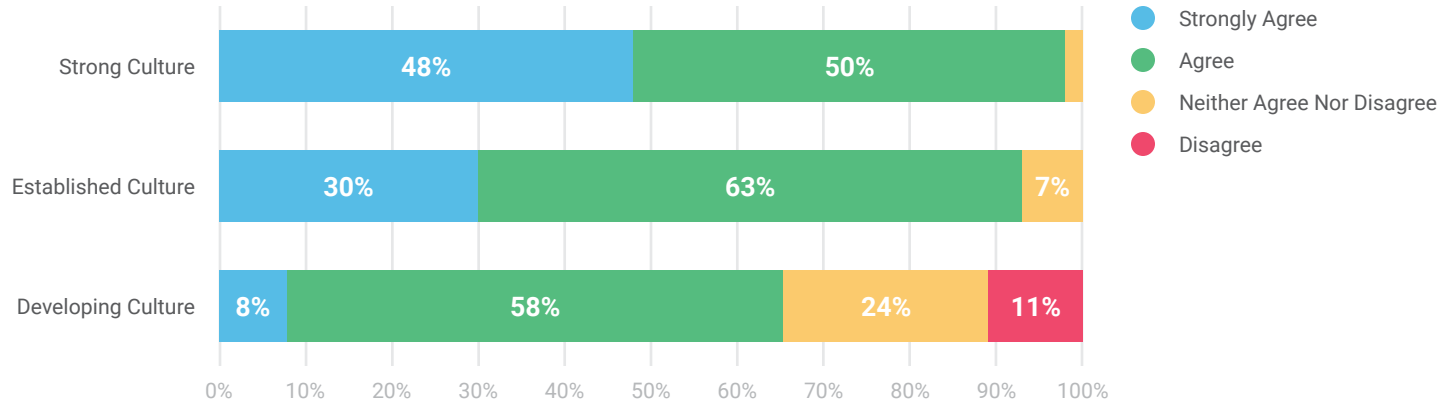
CONFIDENCE IN CYBERSECURITY TRAINING



Culture Impact: Strong Culture Correlates with Higher Confidence

Organizations with a strong cybersecurity culture show the highest confidence in their security awareness training, with nearly all respondents (98%) rating it as effective. In contrast, institutions who view cybersecurity mainly as a compliance task report far lower confidence, underscoring how culture directly shapes training impact.

CYBERSECURITY CULTURE IMPACT ON CONFIDENCE IN TRAINING



Commentary

Regular phishing tests help keep employees alert and prepared, but frequency alone doesn't tell the full story. Institutions who see the strongest results typically pair testing with ongoing, in-depth education, helping staff understand not just the "what" but the "why" behind phishing risks.

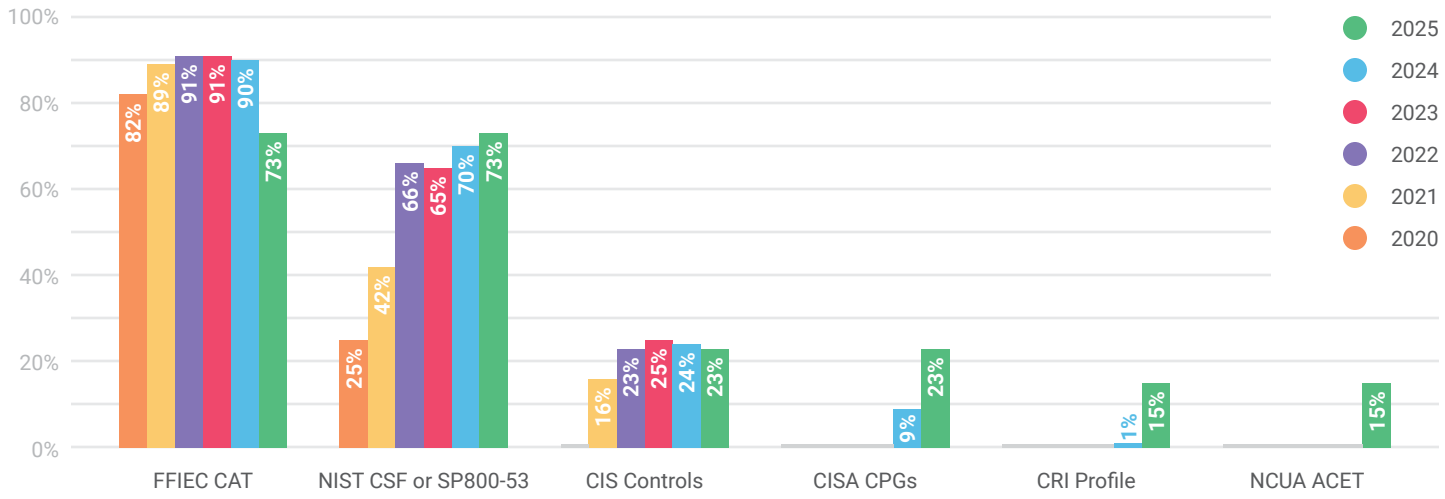
What truly stands out is how much culture drives outcomes. Security awareness isn't just about running tests. It's about fostering a culture where training is valued, reinforced, and tied to the bigger mission of protecting the institution.

Cybersecurity Frameworks & Tools

Observation: The FFIEC CAT is Slowly Being Replaced

On August 29, 2024, the FFIEC announced the sunset of the Cybersecurity Assessment Tool (CAT) effective August 31, 2025. Before this announcement, 90% of institutions were using the FFIEC CAT as their assessment of choice. As of July, when this survey was conducted, 73% of institutions surveyed are using the FFIEC CAT, while other frameworks are beginning to gain popularity.

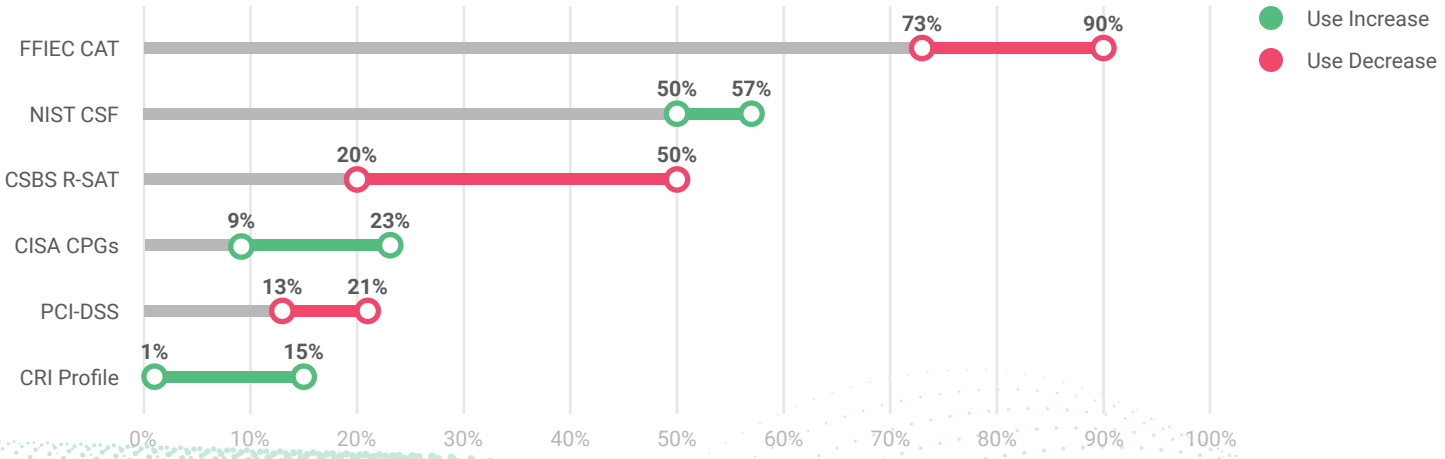
CYBERSECURITY FRAMEWORK USE



Diving Further

While the FFIEC CAT remains the dominant tool for now, most institutions are still in the process of selecting their long-term replacement framework. Below are some of the frameworks that saw the most significant change over the past year.

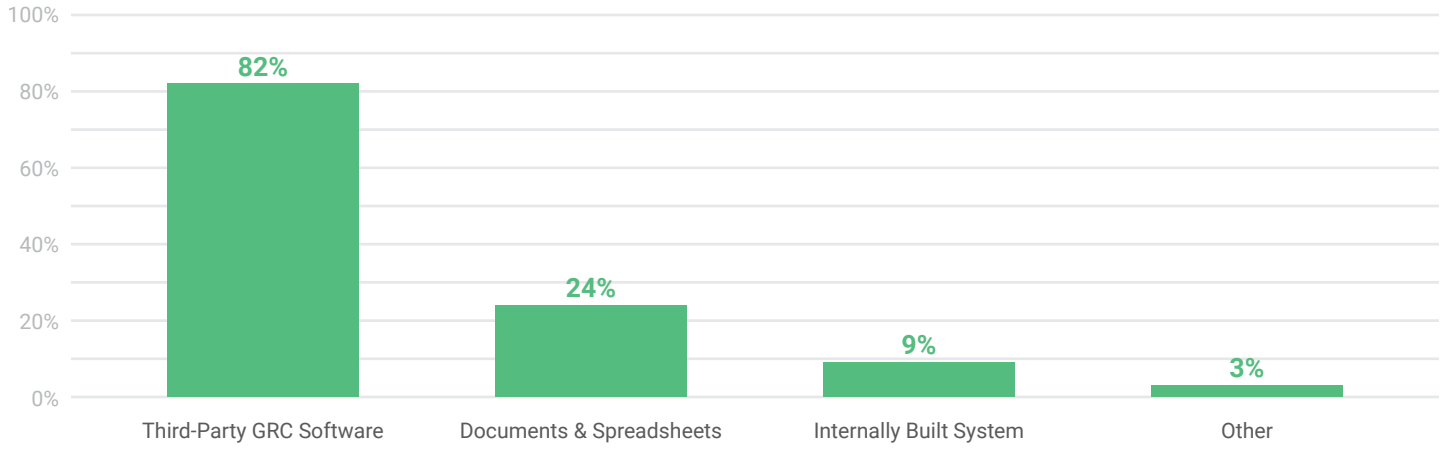
CHANGE IN CYBERSECURITY FRAMEWORK USE



Observation: Large Majority of Institutions Use a GRC Software

When asked how they manage key components of their information security programs (e.g., cybersecurity assessments, risk assessments, policies, vendor management, etc.), 80% of institutions reported using third-party governance, risk management, and compliance (GRC) software, like Tandem, to coordinate these efforts. This high adoption rate underscores the value institutions place on centralized tools to streamline compliance processes, improve oversight, and maintain consistency across their security programs.

INFORMATION SECURITY PROGRAM MANAGEMENT

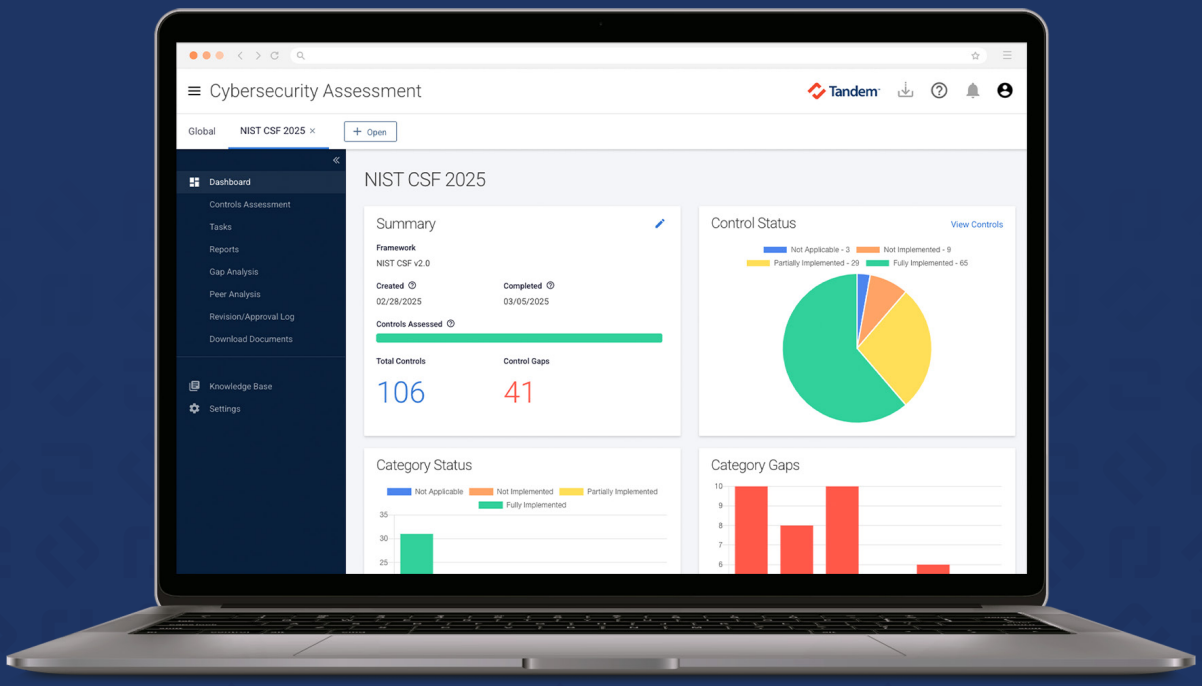


Commentary

The move away from the FFIEC CAT is proving to be a thoughtful, gradual process. Transitioning to a new framework isn't as simple as swapping out a checklist. It means updating processes, retraining teams, and making sure everything stays aligned across the institution. For those still weighing their options, this moment offers a chance to think strategically and select a framework that not only meets compliance needs but also supports long term resilience and growth.

Easily Manage Information Security and Regulatory Compliance

Tandem is information security GRC software trusted by more than 1,700 financial institutions to help keep their information security compliance program efficient and organized. Our team of experts actively monitor and update Tandem with the latest regulatory changes helping you keep your program up-to-date. Tandem is designed specifically for financial institutions (e.g., banks, credit unions, mortgage companies, etc.). It is our goal to help you improve your information security, stay in compliance, and lower overhead costs.



Watch a Demo: Tandem.App/Demo

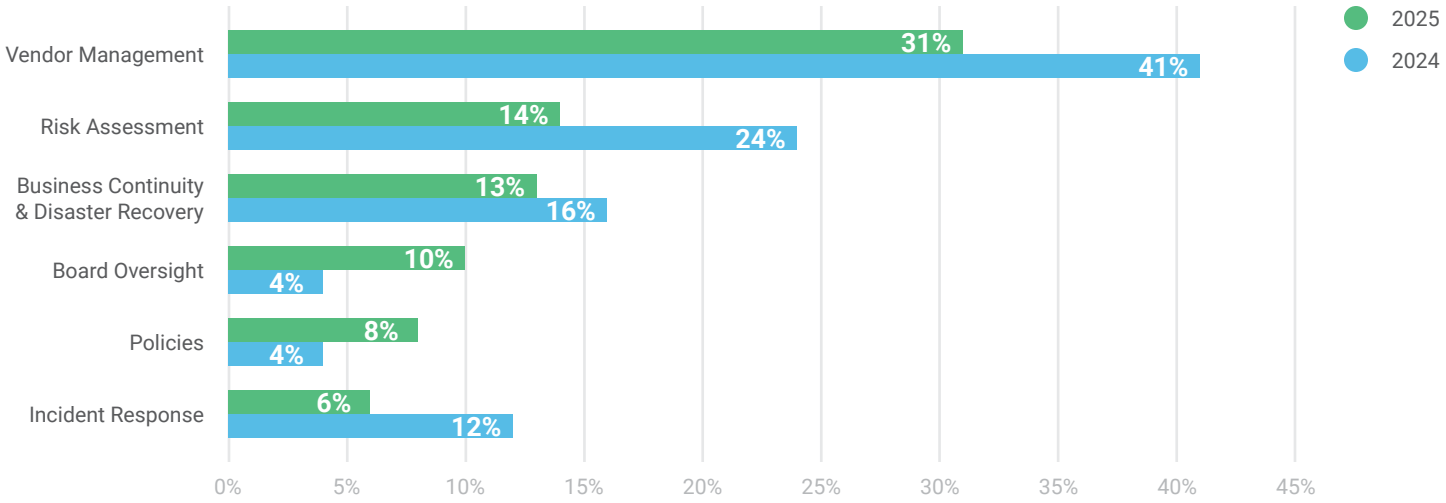
Tandem®

Examination Focus

Observation: Vendor Management Remains the Top Priority

When asked which areas IT examiners focused on, vendor management remained the top concern, though its prominence decreased compared to last year. This shift may indicate a more balanced examination approach in 2025, as 9% of respondents reported there was no particular area of focus during their most recent exam.

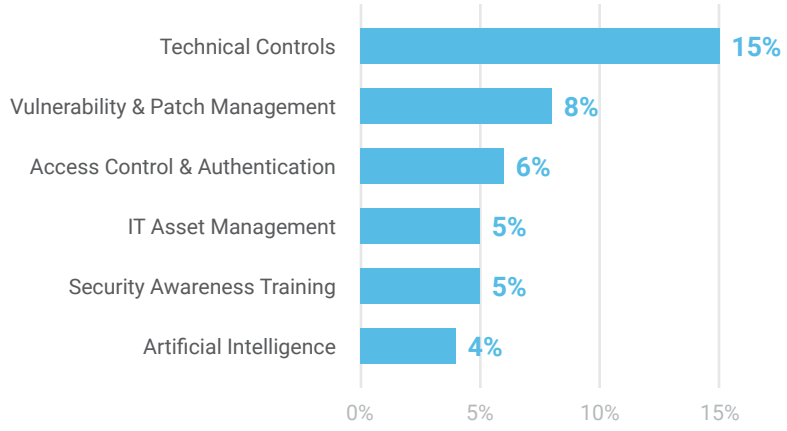
EXAMINER FOCUS DURING LAST EXAM



Observation: Clear Emphasis on Cybersecurity Controls

This year shows a clear emphasis on technical controls like multi-factor authentication (MFA), mobile device management (MDM), data loss prevention (DLP), encryption, network segmentation, and log management. Together with related topics such as artificial intelligence, access control, patching, and IT asset management, the data suggests regulators are looking beyond policies and governance to confirm institutions have concrete security measures in place.

EXAMINER FOCUS DURING LAST EXAM



Commentary

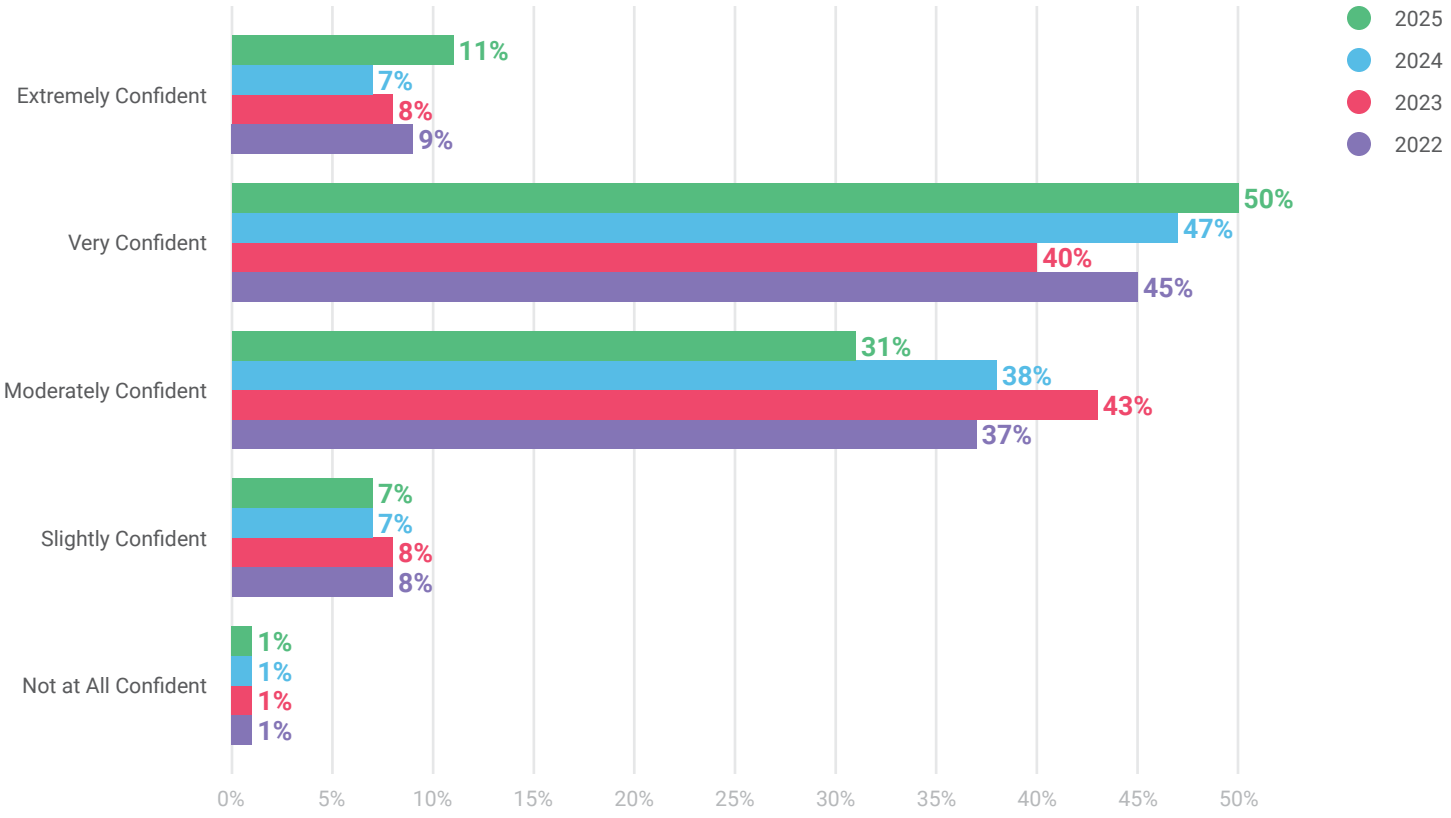
Third-party risk management is still a top focus, though the momentum likely driven by the interagency guidance has begun to settle. With examiners now showing heightened interest in other areas, institutions need to expand exam preparation to ensure security, documentation, testing, and governance practices are strong across the institution.

Incident Response

Observation: Institutions are More Confident in Incident Detection

Respondents are feeling more confident in their cybersecurity posture with 61% saying they are very or extremely confident in their ability to detect an incident as it is happening, compared to 55% in 2024. This upward trend suggests institutions are making measurable progress in strengthening their detection capabilities, likely driven by continued investments in monitoring tools, staff training, and incident response processes.

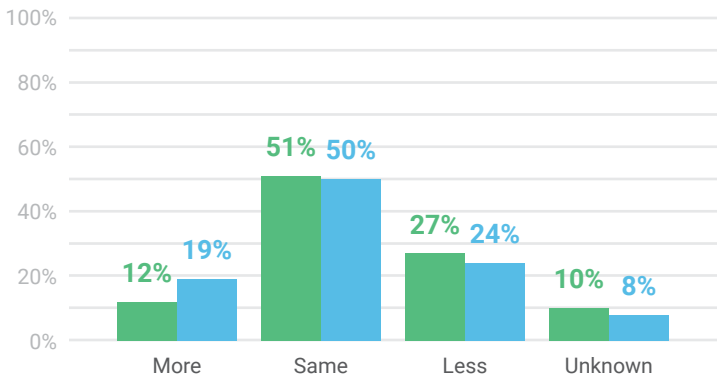
CONFIDENCE IN ABILITY TO DETECT AN INCIDENT



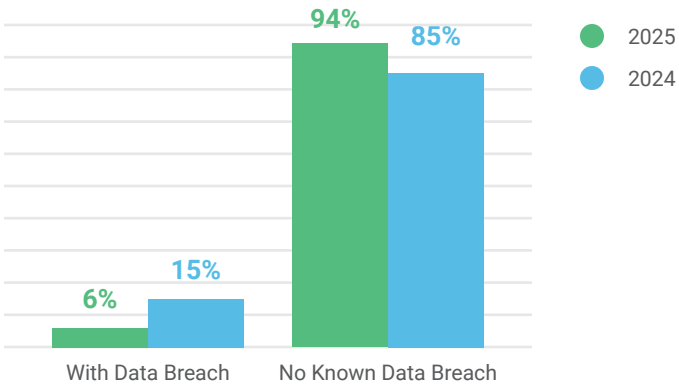
Diving Further

Attacks and known data breaches seem to be on a decline in 2025, with only 12% of institutions stating they are seeing more attacks in 2025 and just 6% reporting a known data breach within the last year. This is down 9% from the prior year.

INCIDENTS COMPARED TO PRIOR YEAR



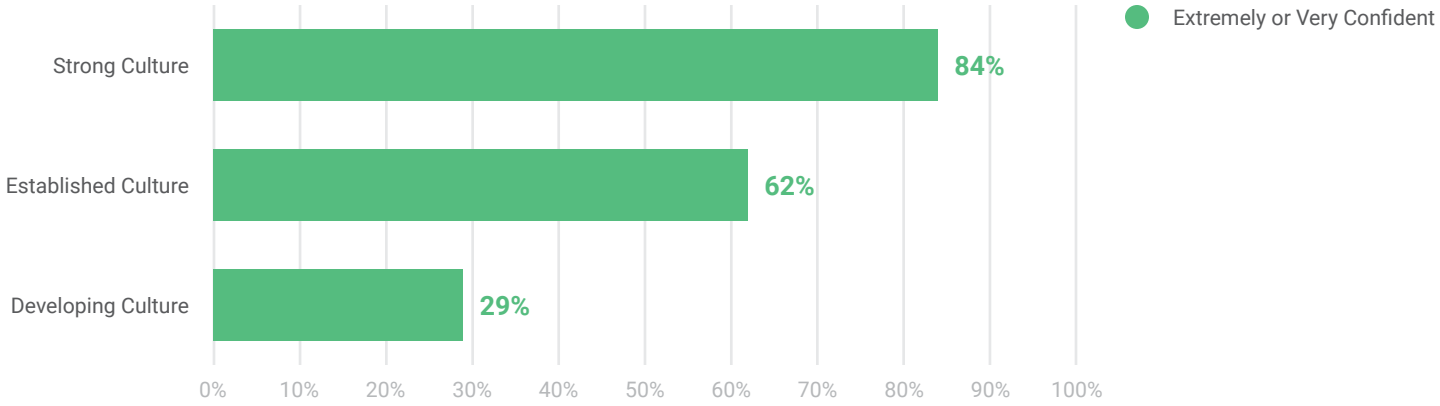
INCIDENTS RESULTING IN DATA BREACH



Culture Impact: Strong Culture Correlates with Incident Detection

Organizations with a strong cybersecurity culture show the highest confidence in their ability to detect an incident with a significant majority of respondents (84%) reporting they feel prepared. In contrast, institutions who view cybersecurity primarily as a compliance requirement report lower confidence (29%), highlighting how culture directly influences detection capabilities and overall readiness.

CYBERSECURITY CULTURE IMPACT ON DETECTING AN INCIDENT



Commentary

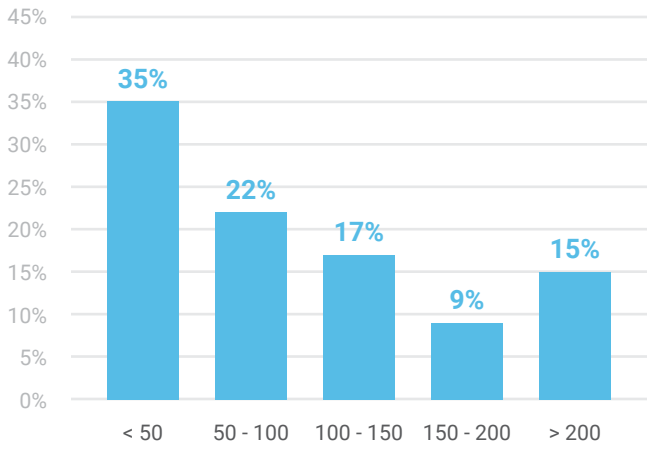
To strengthen incident detection and response, organizations should prioritize building a strong cybersecurity culture with well-trained teams, clear processes, and seamless communication. When people understand their role, they are equipped to detect and respond to threats quickly and effectively, minimizing the likelihood and impact of potential incidents.

Vendor Management

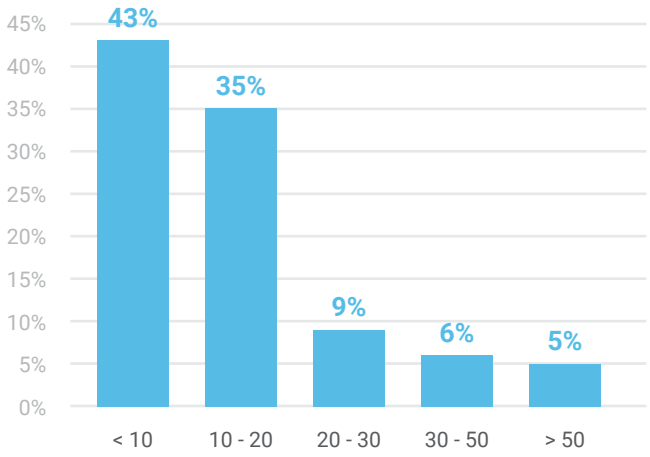
Observation: Institutions Manage an Average of 100 to 125 Vendors

Most institutions manage a large number of vendors, with 41% reporting they oversee 100 or more vendors each year. When it comes to how many vendors are considered critical, 78% of institutions say they have less than 20 critical vendors, with most institutions reviewing their critical vendors on an annual basis.

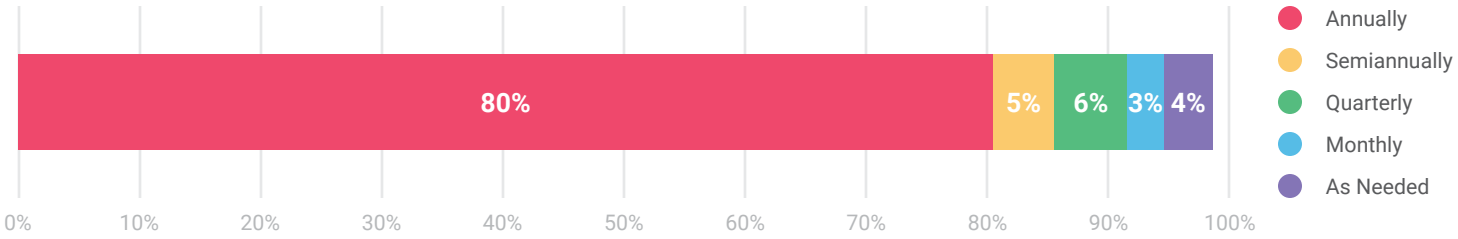
TOTAL VENDORS



CRITICAL VENDORS



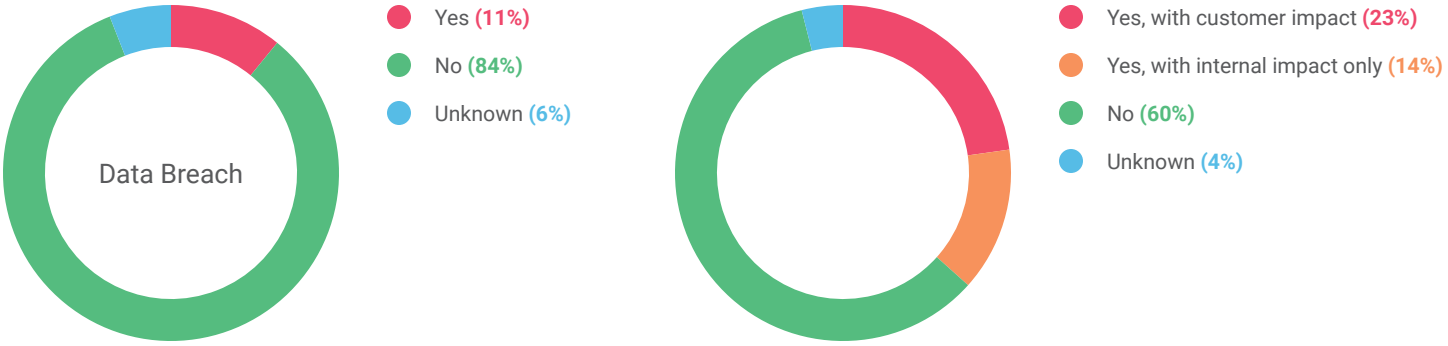
FREQUENCY OF MONITORING CRITICAL VENDORS



Diving Further

When asked about vendor-related security incidents, 84% of institutions reported they have not experienced a confirmed loss or exposure of their own or customers' data due to a vendor, while 11% said they had. In a separate question about operational disruptions within the past 12 months, 23% reported a vendor incident that caused downtime impacting customers, 14% experienced downtime affecting staff only, and 60% said they had no downtime caused by a vendor.

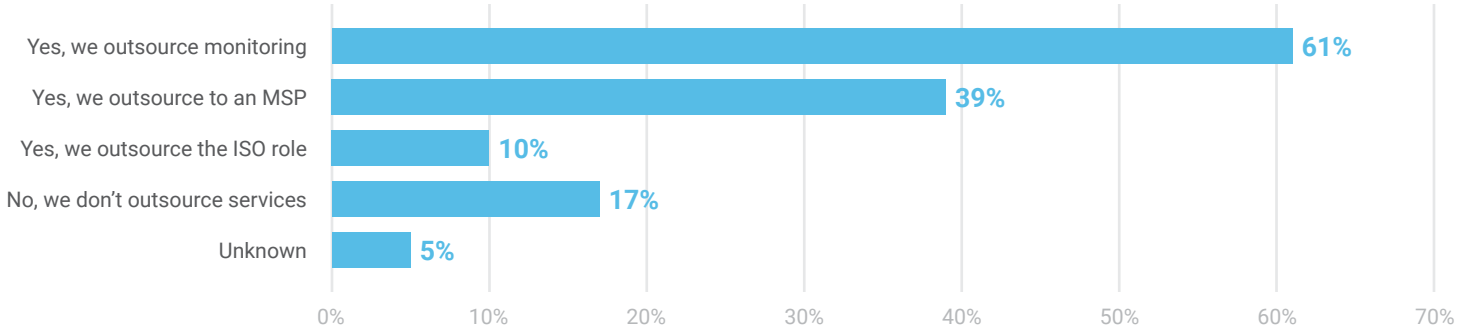
VENDOR-RELATED INCIDENTS



Observation: Vendors Support Key Security Functions

Outsourcing IT and information security functions is increasingly common, with many institutions relying on external monitoring (61%) and managed service providers (39%). However, some functions remain in-house, with only one-in-ten outsourcing the Information Security Officer (ISO) role and 17% managing all security functions internally.

OUTSOURCING INFORMATION SECURITY AND TECHNOLOGY



Commentary

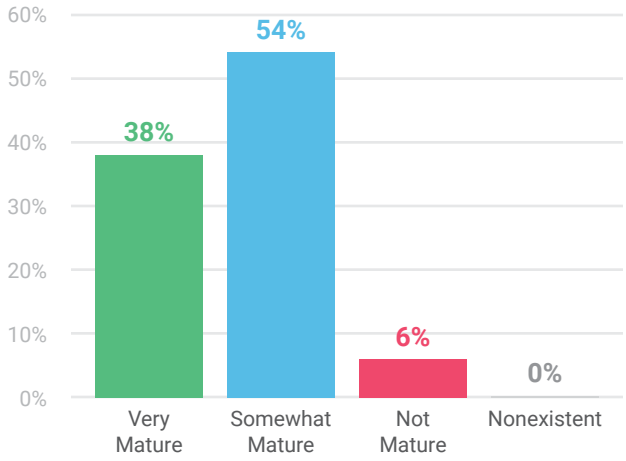
Vendor management continues to be a top priority for financial institutions, driven by the need to prevent data breaches and minimize operational downtime due to third-party incidents. Institutions are strengthening oversight, formalizing processes, and involving experts to address both traditional and emerging risks.

Business Continuity

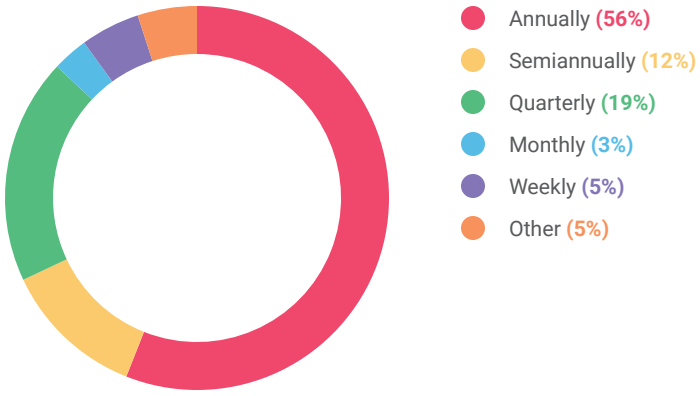
Observation: Most Institutions Have a BCP and Test It Regularly

Most institutions have a business continuity plan (BCP) in place, with 38% describing their plan as mature and regularly tested. Among those who conduct testing, 56% do so at least annually and the rest perform more frequent tests, demonstrating a commitment to ensuring plans remain effective and actionable in the event of a disruption.

BCP MATURITY

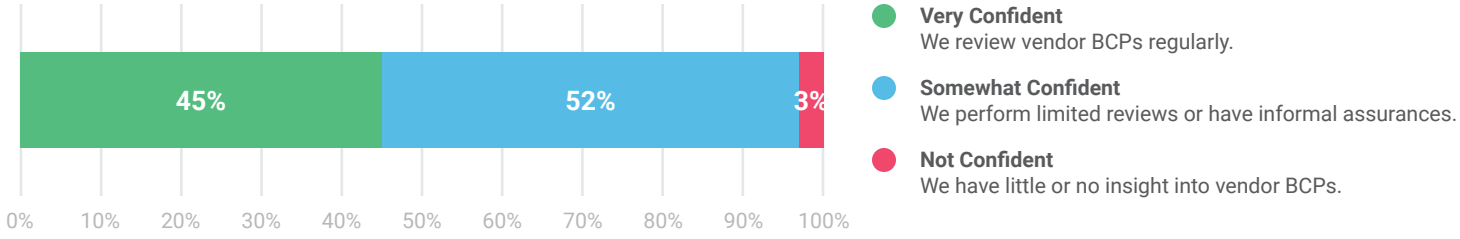


BCP EXERCISE & TEST FREQUENCY



Diving Further

Institutions express strong confidence in their critical vendors' ability to maintain operations during a disruption with 45% reporting they are very confident. Many of these institutions also regularly review their vendors' BCPs.



Commentary

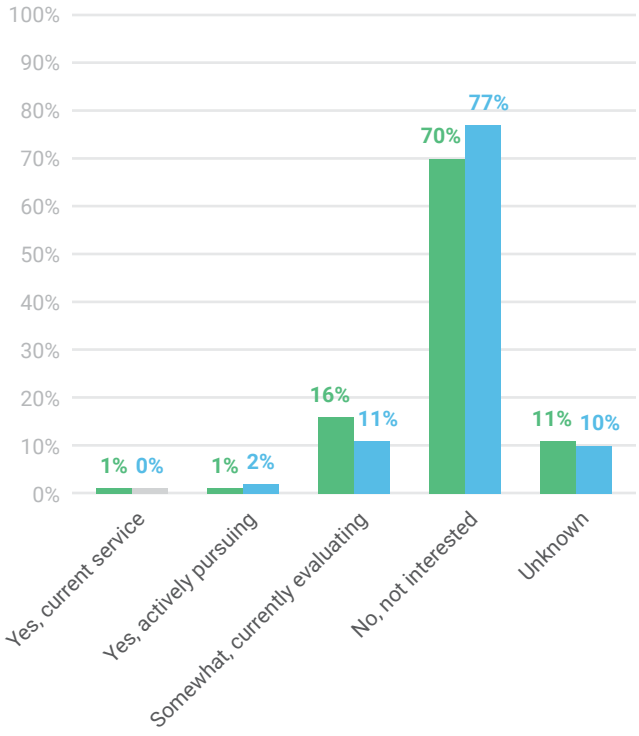
A tested BCP is one of the most valuable tools an organization can have when facing disruption. Regular testing doesn't just check the box; it builds confidence and clarity across teams. However, a "mature" plan isn't static. As operations develop and new risks emerge, a strong BCP is reviewed, updated, and refined with lessons learned from exercises and real-world events. Organizations who view BCP testing as an ongoing process, not just a requirement, are better at adapting quickly and keeping operations running smoothly when an event occurs.

Emerging Technologies

Observation: Cryptocurrency Adoption Remains Low

The adoption of cryptocurrency services has remained relatively consistent. Most (70%) remain uninterested in offering digital asset services. Only a small fraction are actively evaluating or implementing cryptocurrency services. However, there is a 5% increase in institutions who are beginning to evaluate the benefits and risks.

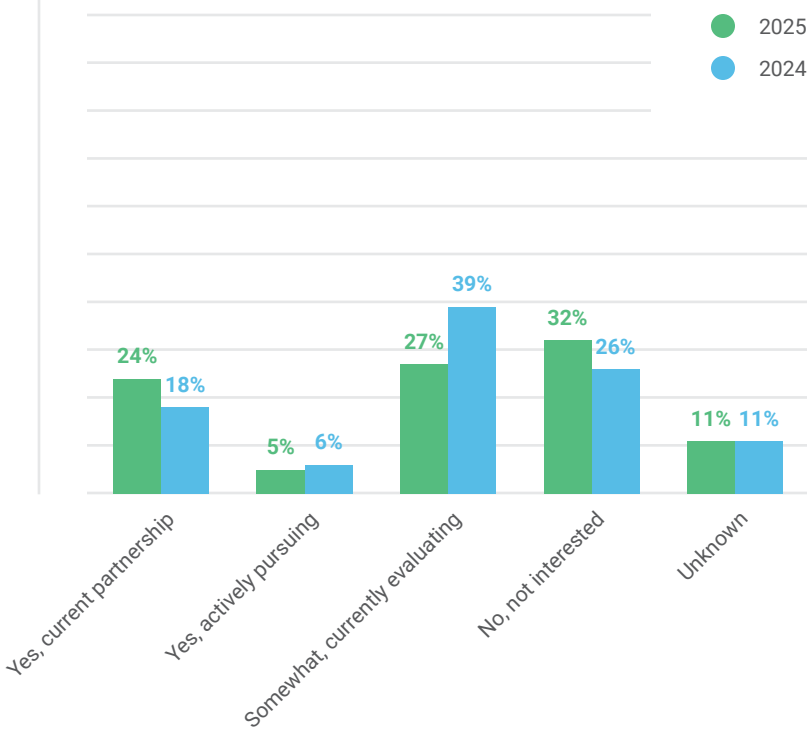
CRYPTOCURRENCY SERVICES



Observation: Fintech Partnerships Slow, but Evaluations Increase

Fintech adoption among institutions shows a shift toward a more cautious, evaluative approach in 2025. While the percentage of institutions currently in a relationship with at least one fintech company decreased from 24% in 2024 to 18% in 2025, those actively evaluating the benefits and risks rose from 27% to 39%.

FINTECH PARTNERSHIPS



Commentary

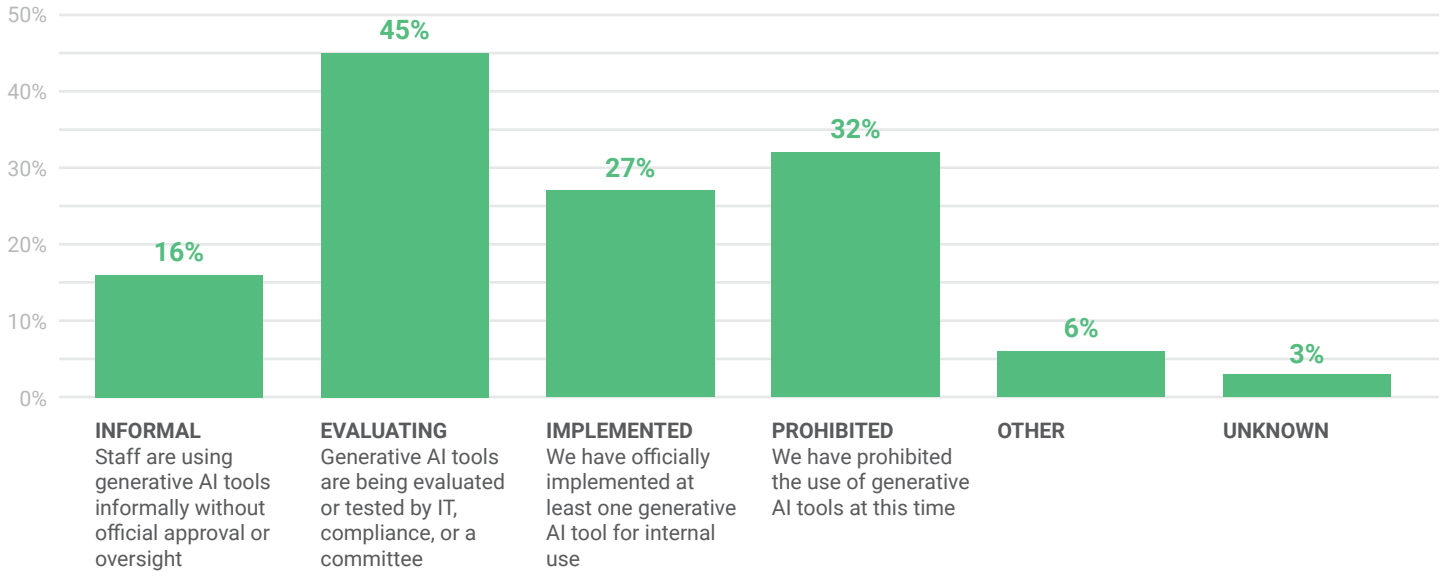
While community financial institutions may not be early adopters, they are purposeful ones. They approach new technologies thoughtfully, often waiting for reliable infrastructure, clear guidance, and real market demand. When emerging technologies are adopted, it's done with a clear focus on enhancing services, improving operations, and supporting core business priorities.

Artificial Intelligence (AI)

Observation: Views on AI Adoption Vary Across Institutions

Generative AI adoption among financial institutions is still emerging. Forty-five percent report AI tools are currently under evaluation, while 27% have officially implemented at least one tool for internal use. Meanwhile, 16% say staff are using generative AI informally without official approval or oversight, and 32% have prohibited their use altogether.

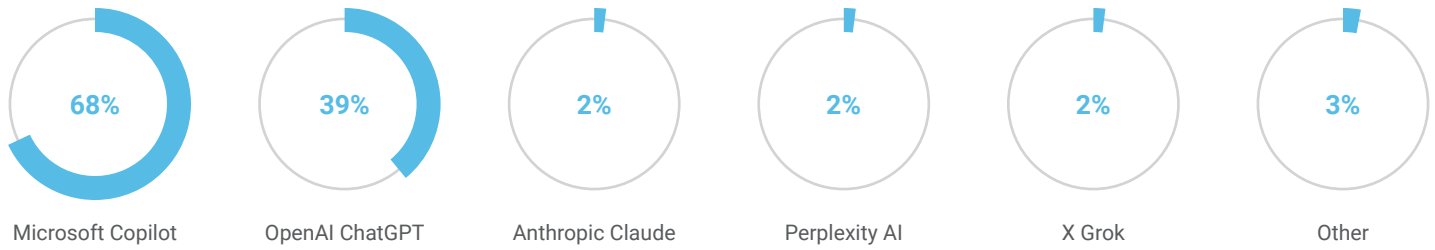
AI USE IN FINANCIAL INSTITUTIONS



Observation: Microsoft Copilot Leads Adoption

Microsoft Copilot stands out as the most widely adopted AI tool, with 68% of respondents reporting use, reflecting its deep integration in financial institution technology environments. ChatGPT follows at 39%, while other tools remain in the low single digits, suggesting they have yet to gain meaningful traction in the industry.

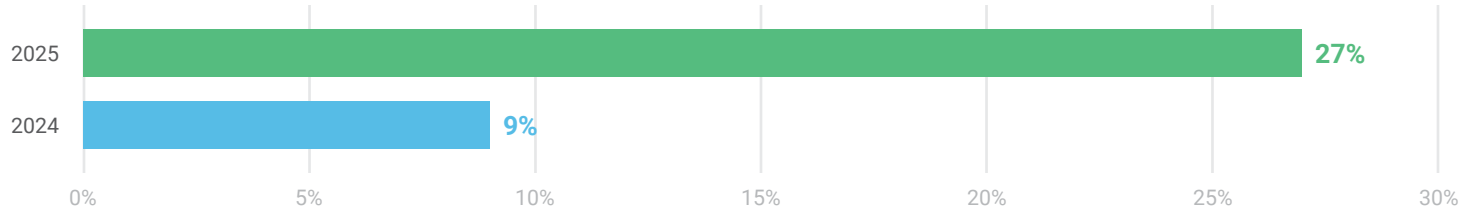
AI TOOL ADOPTION BY FINANCIAL INSTITUTIONS



Diving Further

Official implementation of AI tools rose from 9% in 2024 to 27% in 2025. This three-fold increase suggests that interest is translating into actual adoption in some financial institutions.

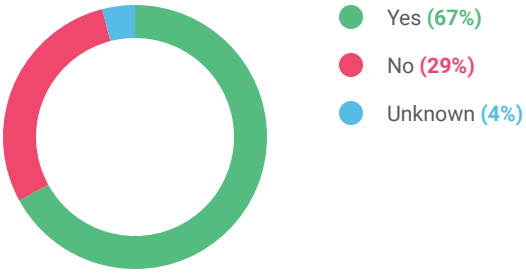
CURRENT USE OF AI TOOLS BY FINANCIAL INSTITUTIONS



Observation: Two-Thirds Evaluate AI in Vendor Management

When asked if they have a formal method to evaluate AI use in vendor products or services as part of their vendor risk management program, 67% of institutions said yes, while 29% said no. This indicates that while a majority are incorporating AI considerations into their vendor oversight processes, nearly one-third have yet to establish a formal evaluation approach for this emerging technology.

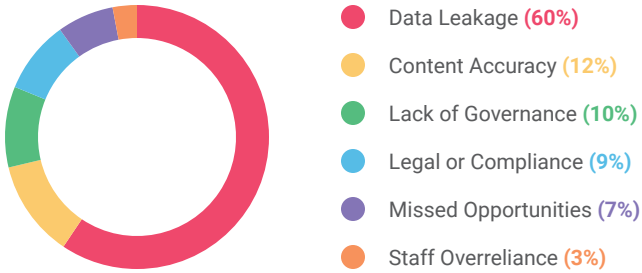
EVALUATION OF AI VENDORS



Observation: Data Leakage is the Biggest Concern

While security involves confidentiality, integrity, and availability, institutions tend to view confidentiality as the most critical concern. Data leakage (60%) far outweighs concerns about content accuracy (integrity) or operational overreliance (availability), underscoring that protecting sensitive information is the top priority.

CONCERNS WITH AI USE



Commentary

The use of AI is rapidly increasing, which brings new layers of risk that can't be overlooked. Without clear policies and oversight, "shadow AI" (when employees use AI tools without approval or monitoring) can create blind spots for security, compliance, and data governance. A well-crafted AI policy helps close these gaps. It can outline acceptable use for employees, guide how to evaluate and monitor AI vendors, and set expectations for security, privacy, and compliance reviews as the technology evolves. Institutions who take this proactive approach can leverage innovation confidently while keeping their operations and data secure.

About the Authors

To learn more about the authors and to book them for a speaking engagement, visit Tandem.App/Speakers.

ALYSSA PUGH, CISM, CRISC
GRC Content Manager

Alyssa is an educator, expert, and content creator with a passion for helping people navigate the challenges of governance, risk management, and compliance (GRC). With more than ten years of experience, Alyssa currently serves as the Tandem GRC Content Manager, where she supervises the content team and oversees the development of educational resources. In addition to her passion for technology, Alyssa is also a wife, graphic designer, and video game enthusiast.

BRIAN WHIPPLE
Marketing Manager

Brian has over ten years of experience in Marketing and is the Marketing Manager for CoNetrix. Since joining the CoNetrix team, Brian has led the company to provide a content-forward strategy by providing educational content on cybersecurity for CoNetrix customers. When not working to provide value for customers, he enjoys spending time with his wife and four children on their small farm.

SAVANNAH RICHARDSON, ITRF
GRC Content Analyst

Savannah finds joy in education - striving to make information more accessible for teaching and sharing resources. She has a B.A. in Business Administration, an M.S. in Finance, and has earned the IT Risk Fundamentals ISACA certificate. Currently, Savannah works as a Software Specialist and is a part of the content team at Tandem. In her free time, Savannah collaborates with a dedicated group supporting small businesses through vendor markets, enjoys reading, and loves to travel.

RUSS HORN, CISA, CISSP, CRISC
President

Russ found a passion for technology at an early age, programming and playing on a Commodore 64. He went on to earn a B.A. in Mathematics and an M.S. degree in Management Information Systems. He spent time as a network administrator, systems analyst, adjunct professor, and IT Auditor prior to serving as President for CoNetrix and Tandem. Along with his interest in technology and cybersecurity, Russ is a husband, father, grandfather, and runner.

LETICIA SAIID, SECURITY+
Chief of Staff & Chief Learning Officer

After earning a B.A. and a M.A. in Mathematics, Leticia joined CoNetrix, where she served as the Tandem Software Support Manager for several years. She built and directed Tandem's first team of support specialists. Leticia now serves as Chief of Staff & Chief Learning Officer where she focuses on corporate strategy, employee development, and training. In her free time she enjoys being a college algebra adjunct professor, playing piano, and solving jigsaw puzzles.

About Tandem

Tandem, LLC is one of four companies owned by CoNetrix, LLC. We develop an online information security governance, risk management, and compliance (GRC) web application designed to ease the burden of regulatory compliance and ultimately, improve your security.

We chose the name Tandem because it works in partnership - in tandem - with you. You bring your knowledge of your organization and your needs, Tandem brings a suite of 11 products built by cybersecurity experts to help you organize and manage your information security program. See how Tandem can help you by visiting Tandem.App.

AUDIT MANAGEMENT
Conduct and respond to audits through a unique framework designed to help you manage, track, and report on the results.

BUSINESS CONTINUITY PLAN
Define and outline plans and procedures to effectively manage operations before, during, and after a disaster.

COMPLIANCE MANAGEMENT
Identify, schedule, and track important compliance projects and deadlines, such as reporting, audits, training, and operations.

CYBERSECURITY ASSESSMENT
Complete cybersecurity control self-assessments based on common frameworks. Report your growth and peer comparison data to management.

IDENTITY THEFT PREVENTION
Create your Identity Theft Prevention Program document, along with customizable employee training for Identity Theft Red Flags.

INCIDENT MANAGEMENT
Prepare for security incidents by developing an incident response plan. When incidents do occur, track and document them throughout your incident handling process.

INTERNET BANKING SECURITY
Create digital banking risk assessment. Offer education with expert-designed security awareness materials.

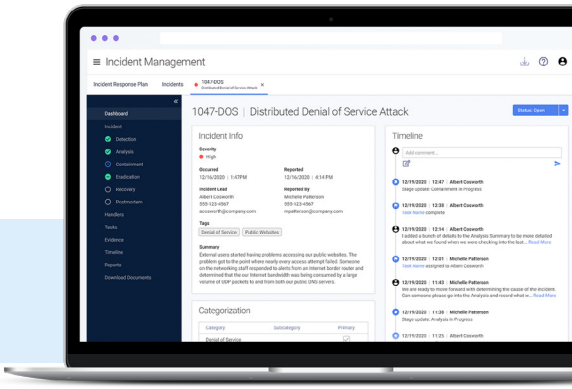
PHISHING
Teach your employees to recognize and avoid social engineering attacks by sending simulated phishing emails and enrolling users in training.

POLICIES
Create and maintain your policies in Tandem. Use our Information Security Policies set, tailored for you through a questionnaire.

RISK ASSESSMENT
Perform information security and asset-based risk assessments with our easy-to-follow format and available templates.

VENDOR MANAGEMENT
Manage contracts, documents, risk assessments, reviews, and other information related to your third-party relationships.

If you would like to learn more about how Tandem can help your organization with cybersecurity and compliance, visit Tandem.App.



Tandem®

info@tandem.app
844-698-9800