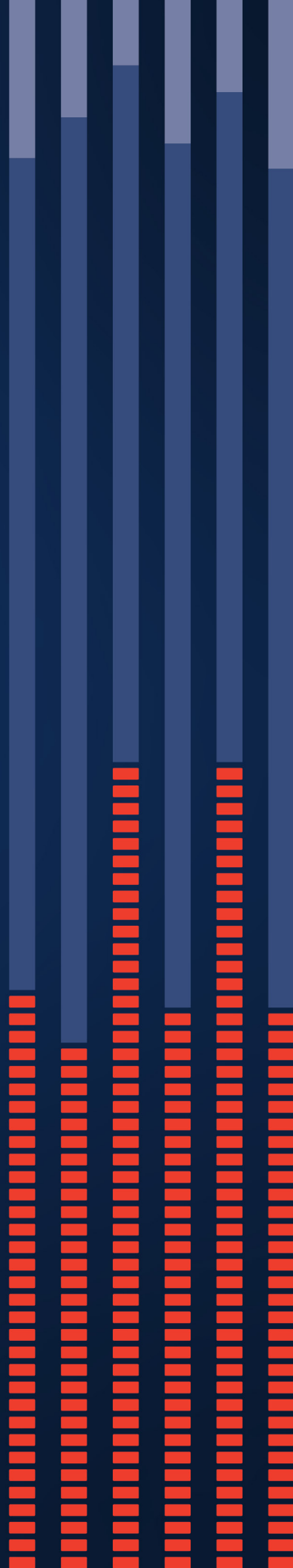


2026

CYBER SECURITY GRC REPORT

FOR THE FINANCIAL INSTITUTION INDUSTRY





About the Cover

In this year's survey, we asked participants to rate the maturity of their cybersecurity governance, risk management, and compliance programs. To reflect the varying levels of maturity across key cybersecurity activities, the cover features an equalizer display. Much like adjusting the levels on a soundboard, institutions continue to strengthen different areas of their programs over time. From left to right, the equalizer bars represent the maturity of business continuity, incident response, information security policies, risk assessments, security awareness training, and vendor management. Learn more about these findings on [Page 17](#).

Contents

Introduction	5
Welcome	5
Demographics	6
Governance	7
Board Oversight	7
Personnel	10
Budgeting	12
Culture	14
Risk Management	16
Program Maturity	16
Security Awareness Training	19
Incident Management	22
Cyber Insurance	27
Vendor Management	30
Artificial Intelligence	34
Compliance	38
Cybersecurity Assessments	38
Examination Priorities	40
Compliance Monitoring	42
Conclusion	44
About the Authors	45
About Tandem	46

Introduction

Welcome

In 2026, cybersecurity governance, risk management, and compliance (GRC) is an ever-moving target for financial institutions. New technologies are moving fast, while legacy systems, long-standing processes, and regulatory expectations still require careful management.

These mixed signals can leave many people wondering:

“Are we the only ones trying to make sense of all this?”

Tandem surveyed more than 300 cybersecurity GRC professionals working at financial institutions across the United States. In our analysis, we saw a clear pattern: community financial institutions are working through many of the same competing priorities, uncertainties, and changes.

This shared experience helped shape our report. What follows is a look at how community financial institutions, like yours, are actually running their cybersecurity programs.

Key Findings

This year’s results point to six recurring themes:

- Programs are broadly mature, but the areas rated lowest are often the hardest ones to validate.
- A strong cybersecurity culture and engaged leadership go hand in hand with healthy programs.
- Small teams carry a wide and growing range of cybersecurity responsibilities.
- Artificial intelligence is now part of daily operations, and with this comes new challenges.
- Third-party risk shows up in maturity ratings, examination priorities, and operational disruptions.
- Cybersecurity framework adoption continues to shift following the FFIEC CAT sunset.

Each theme is explored in the following sections.

Method

Respondents were invited to participate through Tandem’s email communications. Participation was voluntary and respondents were not randomly selected from the industry as a whole.



The survey was conducted between June 1, 2026 and August 3, 2026.



All 306 respondents work for a financial institution based in the United States.

Survey results were reviewed by a team of cybersecurity experts and analysts at Tandem. This report highlights notable trends, changes over time, and meaningful patterns observed in the data. Observations reflect the most significant results and may not include every response option or every comparison analyzed. Percentages are rounded to the nearest whole number, so totals may not always equal 100%.

All findings were self-reported and were not independently verified. As with many survey-based studies, correlations between responses may be influenced by common-method bias, in which a participant’s overall perceptions affect how they respond across multiple questions.

Year-over-year comparisons draw on separate samples in each survey year and may reflect differences in respondent composition, as well as underlying changes in industry practices.

How to Read This Report

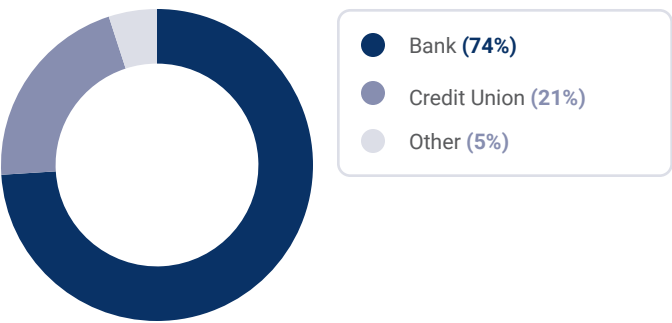
This report is organized around the three functions of a cybersecurity program: governance, risk management, and compliance. Within each topic, you’ll find three recurring elements.

- **Observation**
An overview of direct findings from the results.
- **Tuning In**
Insights to highlight trends and cross references.
- **Takeaway**
Practical recommendations to cut through the noise.

Demographics

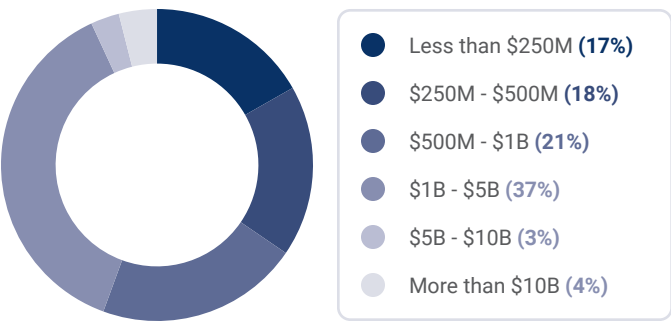
Institution Types

Of those who responded, 74% work for a bank, 21% work for a credit union, and the remaining respondents work for other financial institutions (e.g., farm credit institutions, mortgage companies, trust companies).



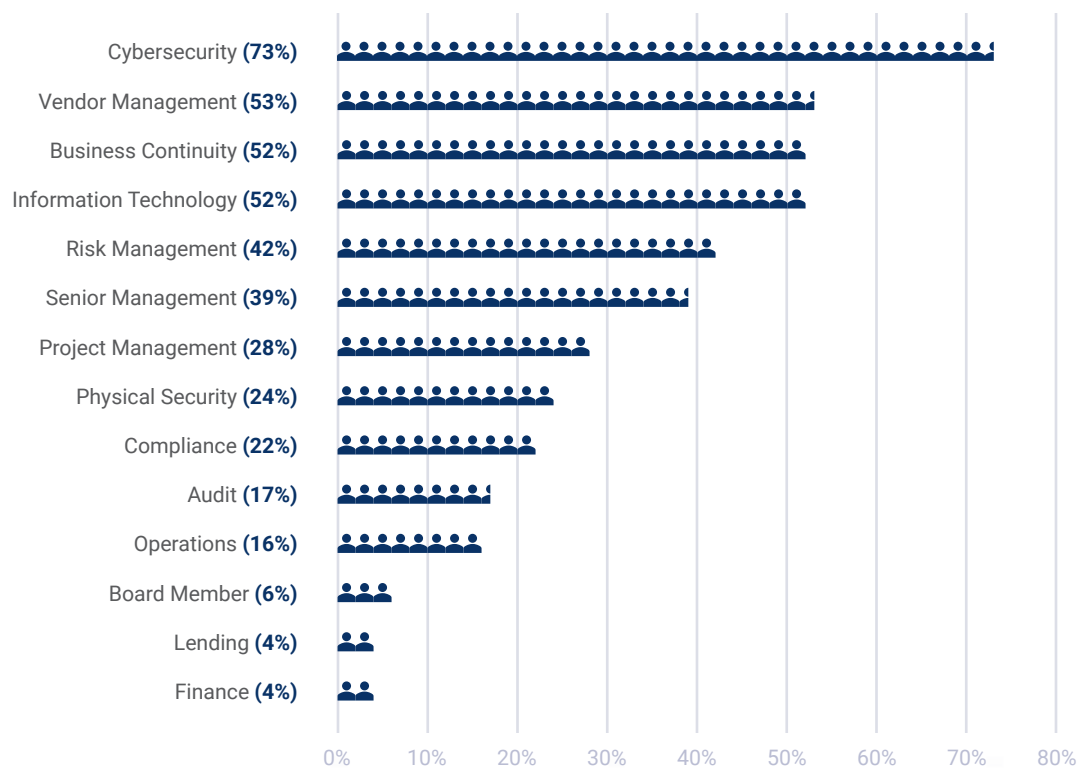
Asset Sizes

Survey respondents represented a wide range of institution sizes. A majority (56%) came from institutions with less than \$1 billion in assets, while 44% were from institutions with \$1 billion or more in assets.

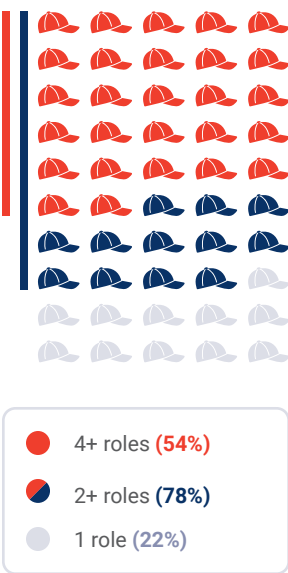


Roles & Responsibilities

Survey respondents worked primarily within cybersecurity / information security, vendor management, business continuity, and information technology roles. Respondents were asked to select all that applied.



Most cybersecurity GRC professionals wear many hats. Nearly four in five respondents (78%) reported holding two or more roles, and more than half (54%) selected four or more.



Governance

In the context of this report, governance refers to how a financial institution directs, supports, and oversees its cybersecurity program. Looking at trends in Board oversight, personnel, budgeting, and culture provides some of the clearest signals about an institution’s cybersecurity posture.

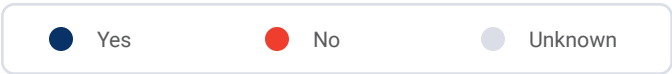
Board Oversight

The Board of Directors is ultimately responsible for overseeing the institution’s cybersecurity program and ensuring risk is managed in a safe and sound manner. To better understand how this responsibility is carried out in practice, we looked at trends in cybersecurity experience and reporting cadence.

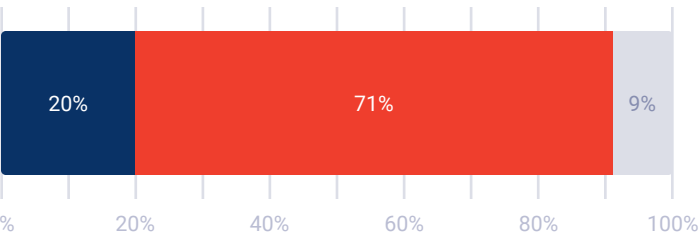
Observation

Most Boards lack a director with cyber experience.

71% of survey respondents reported their institution’s Board of Directors does not include a director with formal cybersecurity qualifications or expertise, such as relevant professional experience, certifications, or academic credentials.



BOARD MEMBER CYBER EXPERIENCE

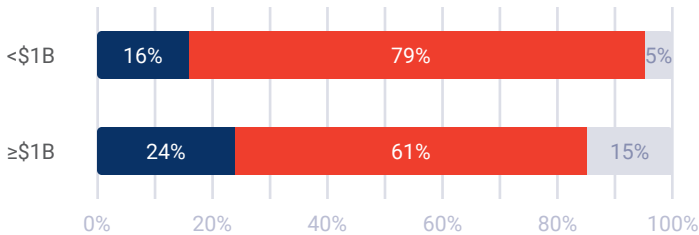


Tuning In

Among institutions with less than \$1 billion in assets, 16% reported having a director with formal cybersecurity qualifications or expertise, compared to 24% of institutions with \$1 billion or more in assets.

While most institutions in both groups reported lacking cybersecurity expertise on the Board, larger institutions were more likely to report having Board members with experience.

CYBER EXPERIENCE BY ASSET SIZE

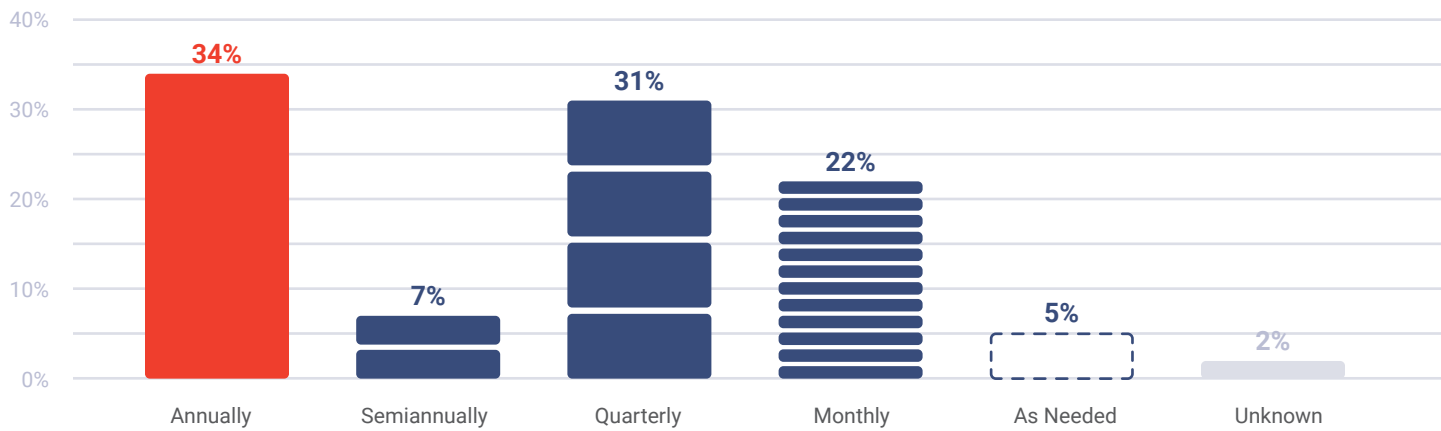


Observation

Board cybersecurity reporting occurs regularly.

Reporting is an important part of Board oversight, as it is how most Boards stay informed of cybersecurity updates. Annual reporting was the most common individual cadence, cited by 34% of respondents. However, more than half of institutions (53%) reported providing cybersecurity updates at least quarterly, indicating many Boards receive information more frequently than once per year.

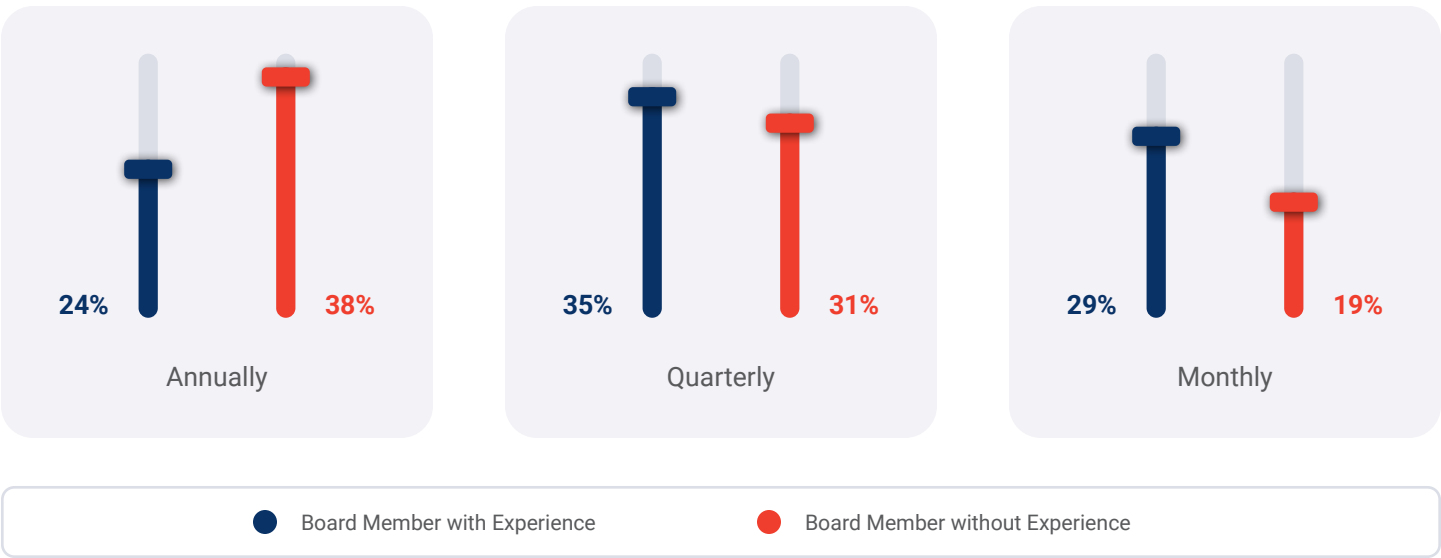
BOARD CYBERSECURITY REPORT FREQUENCY



Tuning In

Institutions with at least one Board member who has formal cybersecurity experience tend to report cybersecurity information more frequently. Among institutions with Board-level cybersecurity expertise, 64% report to the Board quarterly or monthly, compared to 50% of institutions without such expertise.

REPORT FREQUENCY BY BOARD MEMBER CYBERSECURITY EXPERIENCE



Takeaway

While the survey results do not establish causation, they do suggest a meaningful relationship between Board cybersecurity expertise and cybersecurity oversight.

- **Institutions with at least one Board member who has cybersecurity expertise** were more likely to report to the Board quarterly or monthly. While this isn't a surprising finding, it does indicate Board members with cybersecurity backgrounds may be more comfortable engaging in conversations about cyber risk, asking informed questions, and encouraging regular discussions about cybersecurity.
- **Institutions without Board members who have cybersecurity expertise** are in good company. Most survey respondents reported their Boards do not include cybersecurity experts, especially among smaller community institutions. In those cases, management often helps fill the gap by providing reporting that translates cybersecurity activities, risks, and priorities into terms directors can use for decision-making.

At the end of the day, cybersecurity expertise may help directors engage more confidently in cybersecurity discussions, but effective oversight starts with Board members who stay informed, ask questions, and remain engaged in cybersecurity discussions.

Board Member Resource

Want to help your Board get more value from cybersecurity reporting? Download our resource, *A Board Member's Guide to Cybersecurity Assessments*, to learn how directors can interpret assessment results, ask better questions, and confidently oversee cybersecurity risk regardless of which framework your institution uses.

Download the Resource: Tandem.App/Board



Personnel

Staffing plays a key role in cybersecurity governance, shaping how the institution’s cybersecurity program is implemented and managed. To better understand how institutions resource these efforts, we looked at trends in staffing levels and expected changes to cybersecurity personnel over the next 12 months.

Observation

Cyber programs are often supported by small teams.

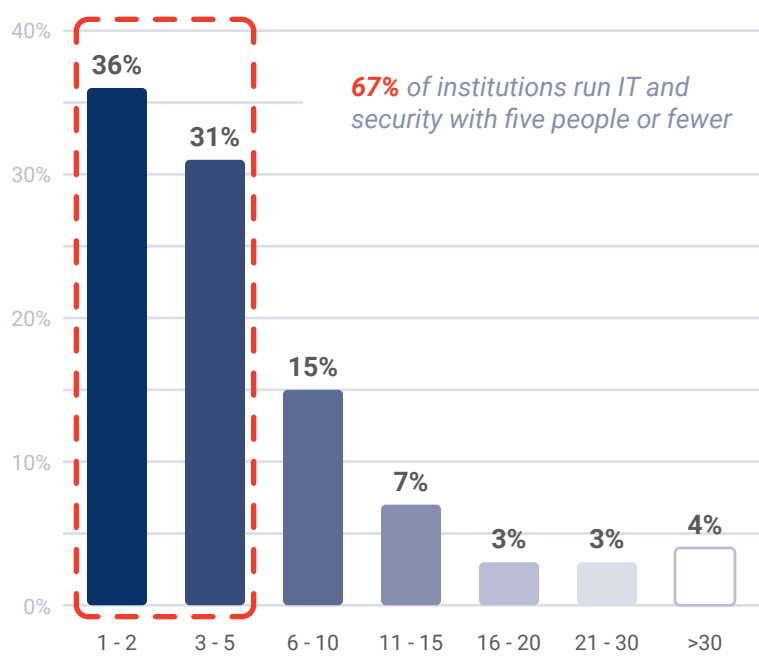
Over a third (36%) of survey respondents reported relying on just one or two full-time IT, information security, and cybersecurity professionals.

Two-thirds of respondents (67%) reported having five or fewer and a significant majority of institutions (82%) reported employing 10 or fewer full-time staff supporting these functions.

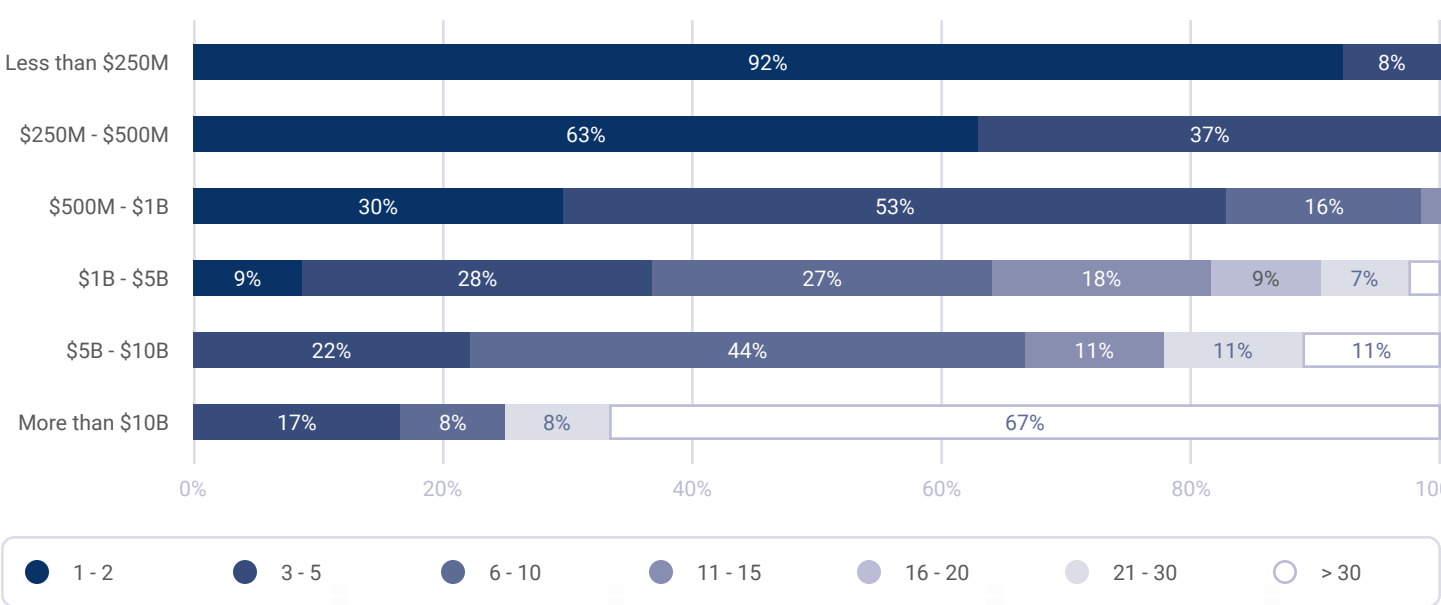
Tuning In

Cybersecurity staffing generally grows alongside the size and complexity of the institution. Institutions with less than \$250 million in assets overwhelmingly reported having one to two full-time IT, cybersecurity, and information security professionals, while larger institutions were more likely to report larger teams. Institutions with \$1 billion or more in assets were far more likely to report staffing levels above 10 employees.

NUMBER OF FULL-TIME STAFF



FULL-TIME STAFF BY ASSET SIZE

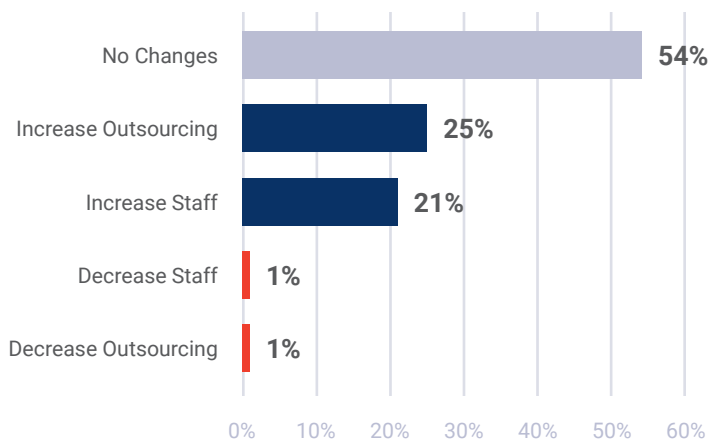


Observation

Staffing is expected to remain stable or grow.

More than half of institutions (54%) expect no planned changes to their cybersecurity staffing and outsourcing model over the next year. Among those anticipating changes, expansion is the major theme, whether through additional employees (21%) or greater reliance on outsourced services (25%).

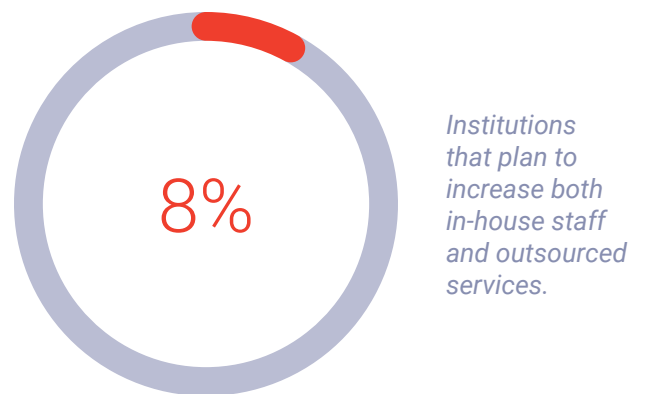
ANTICIPATED STAFFING CHANGES



Tuning In

Among respondents who selected more than one answer option, the only combination reported at meaningful levels was increasing both in-house staff and outsourced services (8%). This suggests that when institutions anticipate changes to both staffing models, they are more likely to expand both internal and external resources, rather than choose one over the other.

MULTIPLE CHANGES



Takeaway

The survey data paints a picture of an industry that wants to do more with the resources it currently has. While some institutions are preparing to grow by adding staff or expanding outsourced support, most expect their cybersecurity staffing model to look much the same a year from now.

This reality creates two different challenges:

- **Institutions planning to grow** must determine where additional people or services will have the greatest impact, often combining internal personnel who bring organizational expertise with outsourced providers who bring specialized expertise and capacity.
- **Institutions planning to maintain** must carefully balance day-to-day operational responsibilities with strategic cybersecurity initiatives, making intentional decisions about where time and resources are invested.

In both cases, what matters most is not the size of the team, but whether the institution has the right personnel resources to effectively manage cybersecurity risk.

Budgeting

Budgeting provides insight into how institutions prioritize and fund cybersecurity initiatives. To better understand how financial institutions manage their budgets, we looked at how cybersecurity funding is allocated and how institutions expect their IT and cybersecurity budgets to change in the future.

Observation

Cyber funding is typically integrated with IT budgeting.

Most institutions fund cybersecurity through their broader IT budgeting process. A majority of respondents (62%) reported that cybersecurity funding is included within the IT budget, either as a defined line item (28%) or without being tracked separately (34%). Only 14% of institutions maintain a dedicated cybersecurity budget separate from IT.

CYBERSECURITY FUNDING MODEL

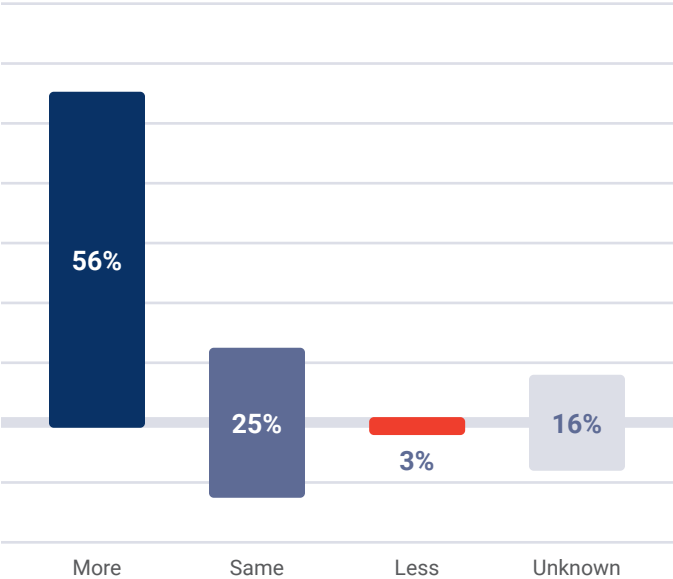
14%	Dedicated Cybersecurity Budget
28%	Dedicated Line Item in IT Budget
34%	Funding Included in IT Budget
7%	As-Needed Funding for Major Projects
8%	No Formal Funding or Budget
9%	Unknown

Observation

Most institutions expect cyber budgets to increase.

More than half of respondents (56%) reported their institution's 2026 cybersecurity budget was, or was expected to be, higher than in 2025. An additional 25% reported spending was expected to remain about the same, while only 3% anticipated a decrease.

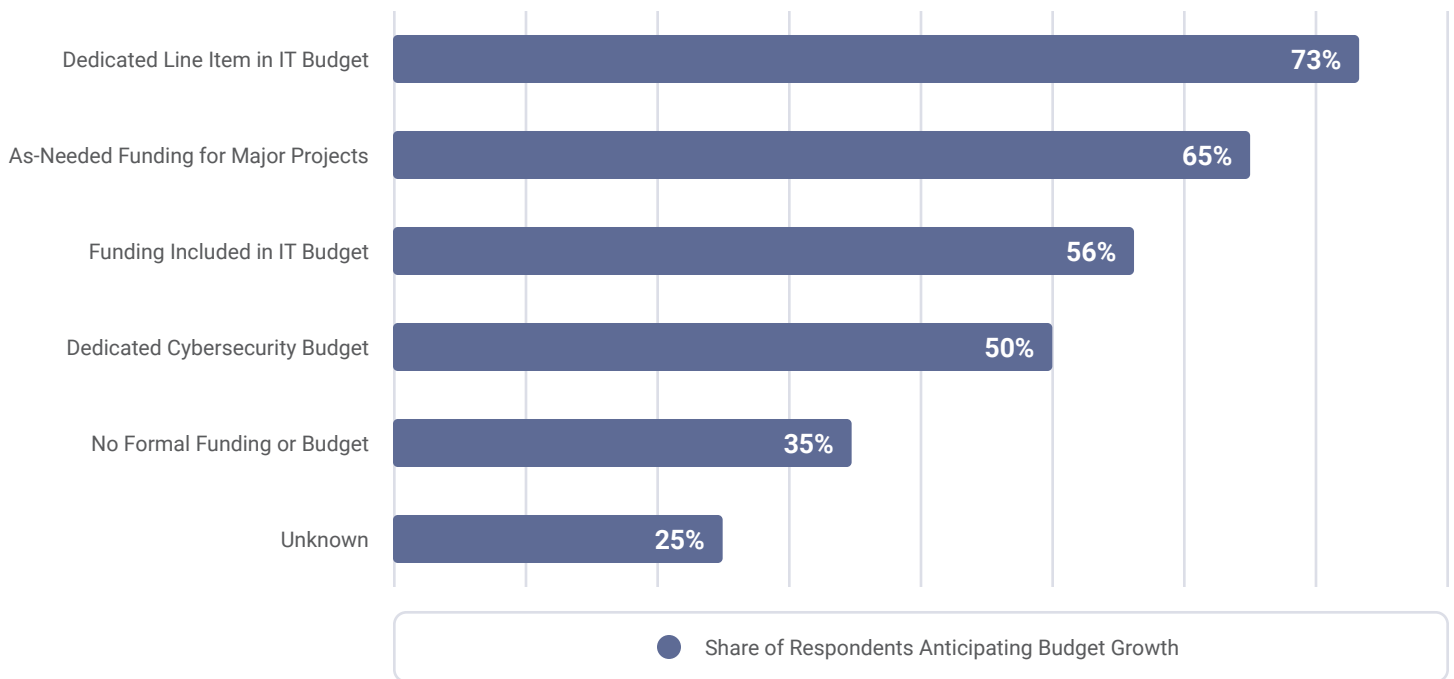
ANTICIPATED BUDGET CHANGES



Tuning In

Institutions with an established path for cybersecurity funding were more likely to expect budget growth than those without one. Growth expectations peaked among institutions that track cybersecurity as a defined line item within the IT budget (73%). That compares with 56% of those that include it in the IT budget without tracking it separately, and 35% of those with no formal cybersecurity budget.

LIKELIHOOD OF BUDGET GROWTH BY CURRENT FUNDING MODEL



Takeaway

For many financial institutions, the survey data shows cybersecurity investments are commonly planned and funded alongside other technology priorities. In practice, this integrated approach can provide several benefits.

- It reinforces that cybersecurity is a core technology investment.
- It reflects the overlap between IT and cybersecurity spending.
- It streamlines technology planning and investment decisions.

However, integrated budgeting can also make cybersecurity priorities less visible. Regardless of how cybersecurity spending is categorized, institutions should ensure cybersecurity needs are considered alongside other technology priorities when investment decisions are made.

Culture

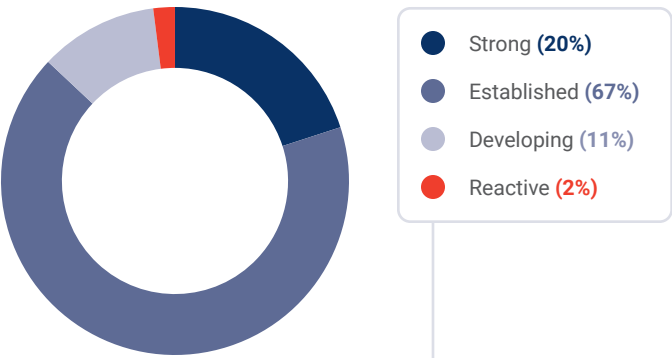
Leadership sets the tone at the top, and that tone helps shape cybersecurity culture. To better understand this relationship, we looked at how respondents describe their institution’s cybersecurity culture and how those perceptions align with confidence in the institution’s overall cybersecurity posture.

Observation

Most institutions report an established cyber culture.

While 20% of respondents reported a strong culture in which cybersecurity is deeply embedded throughout the organization, the largest group (67%) described an established culture, where cybersecurity receives consistent attention and support. The remainder (13%) reported a developing or reactive culture.

CYBERSECURITY CULTURE

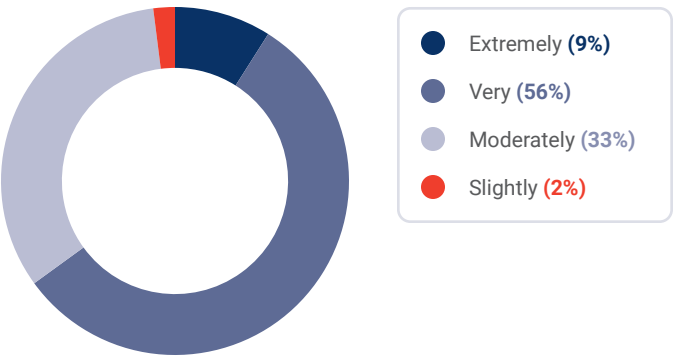


Observation

Most are also confident in their cybersecurity posture.

Nearly two-thirds of respondents (65%) reported being extremely or very confident in their institution’s cybersecurity posture, with another third indicating moderate confidence. Only a small minority expressed low confidence, suggesting most institutions view their cybersecurity program positively.

CYBERSECURITY POSTURE CONFIDENCE



What We Mean by “Culture”

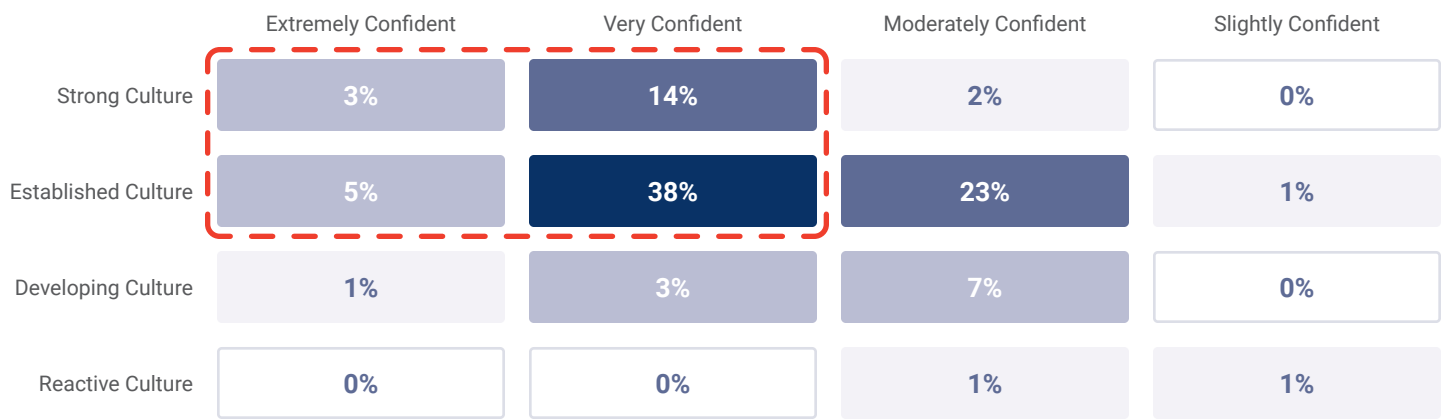
When respondents answered the question about culture, the following definitions were used.

- **Strong Culture.** Cybersecurity is deeply embedded in our culture. We integrate it into planning, budgeting, and daily operations, and it plays a central role in organizational strategy.
- **Established Culture.** Cybersecurity is important and well-supported. We consistently invest attention and resources into cybersecurity, though it is not a primary driver of organizational strategy.
- **Developing Culture.** Cybersecurity is necessary for compliance. We focus on meeting regulatory and examiner expectations while managing operational risk effectively.
- **Reactive Culture.** Cybersecurity is treated as an operational necessity. We address cybersecurity needs only in response to business requirements or specific events.

Tuning In

Respondents who reported high confidence (i.e., Extremely Confident or Very Confident) in their cybersecurity posture also strongly tended to define their cybersecurity culture as strong or established. Together, these groups accounted for 60% of all survey responses, compared to just 4% for institutions with developing cultures and virtually none for those reporting a reactive culture.

CULTURE AND CONFIDENCE



Takeaway

While things like culture and confidence may be difficult to quantify, the survey results suggest a meaningful relationship between the two. Institutions with a strong culture were also much more likely to express high confidence in their cybersecurity posture.

- **For institutions with a “Strong” or “Established” culture**, it is important to maintain momentum. Culture is not a permanent achievement or something to recertify annually. Continue to revisit the priorities and practices that helped build a positive cybersecurity culture in the first place.
- **For institutions with a “Developing” or “Reactive” culture**, small improvements can have a big impact. Integrating cybersecurity concepts into day-to-day decision-making and business processes can help strengthen culture over time and encourage more consistent awareness of cybersecurity across the institution.

Cybersecurity culture influences how people prioritize and discuss cybersecurity issues. While it may be a softer metric than budgets or staffing, it remains an important part of an institution’s cybersecurity program governance.

Risk Management

In the context of this report, risk management refers to how an institution identifies, assesses, and responds to cybersecurity risk. Looking at trends in program maturity, training, incident response, vendor management, and emerging risks provides some of the clearest signals about an institution’s ability to manage risk effectively.

Program Maturity

A cybersecurity program provides the structure through which institutions manage and oversee cybersecurity risk management activities. To better understand program development and maturity, we looked at how respondents manage their cybersecurity program and assess their progress.

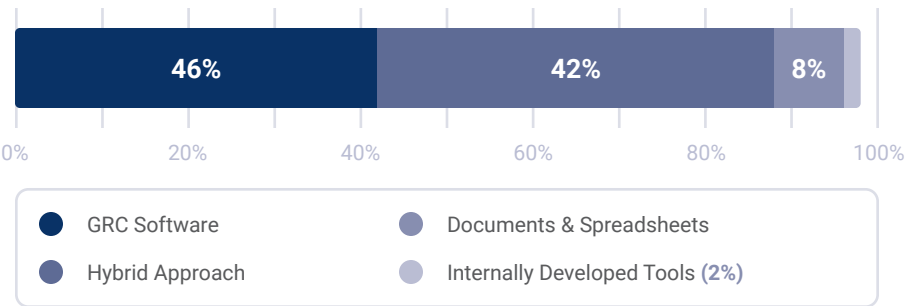
Observation

Cyber programs are managed formally.

Nearly all respondents reported having a formal method for managing their cybersecurity program.

Dedicated GRC software and hybrid approaches account for the vast majority of responses (88%), while only 8% reported sole reliance on documents and spreadsheets.

PROGRAM MANAGEMENT METHODS

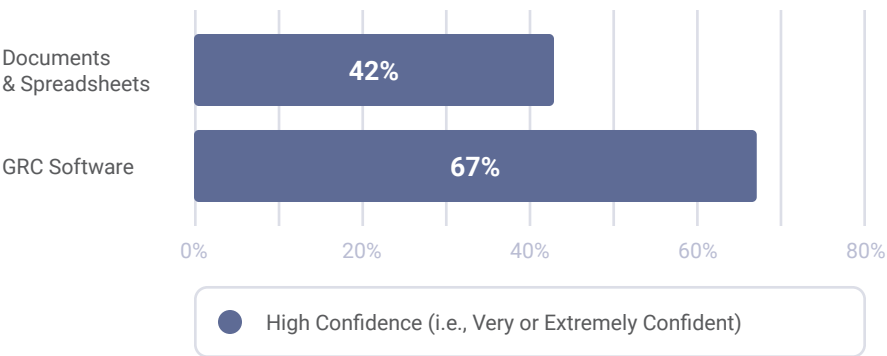


Tuning In

The use of software-supported program management was consistent across institution types and asset size. Approximately 89% of banks and 85% of credit unions reported using either third-party GRC software or a hybrid approach.

Institutions relying solely on documents and spreadsheets reported lower confidence in their overall cybersecurity posture; however, these results do not establish a direct relationship between the tools used and overall confidence.

CONFIDENCE BY PROGRAM MANAGEMENT METHOD

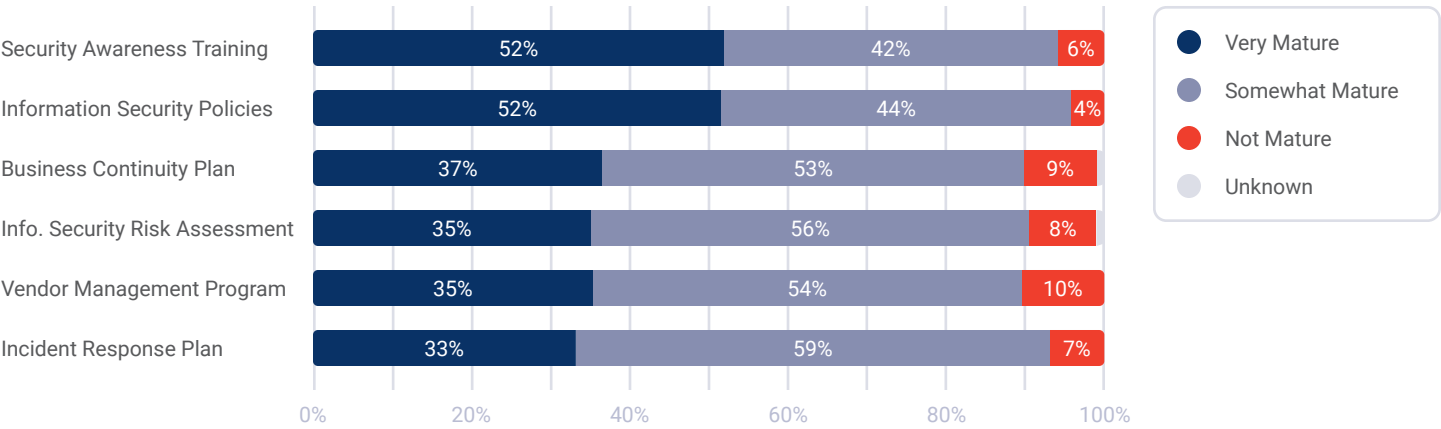


Observation

Cybersecurity program components are well established with room to grow.

Respondents generally reported strong levels of maturity across key cybersecurity program components. Between 89% and 96% rate each component as either somewhat or very mature. Security awareness training and information security policies (52%) received the highest “very mature” ratings, while information security risk assessment and vendor management programs (35%), and incident response plans (33%) were less frequently viewed as very mature.

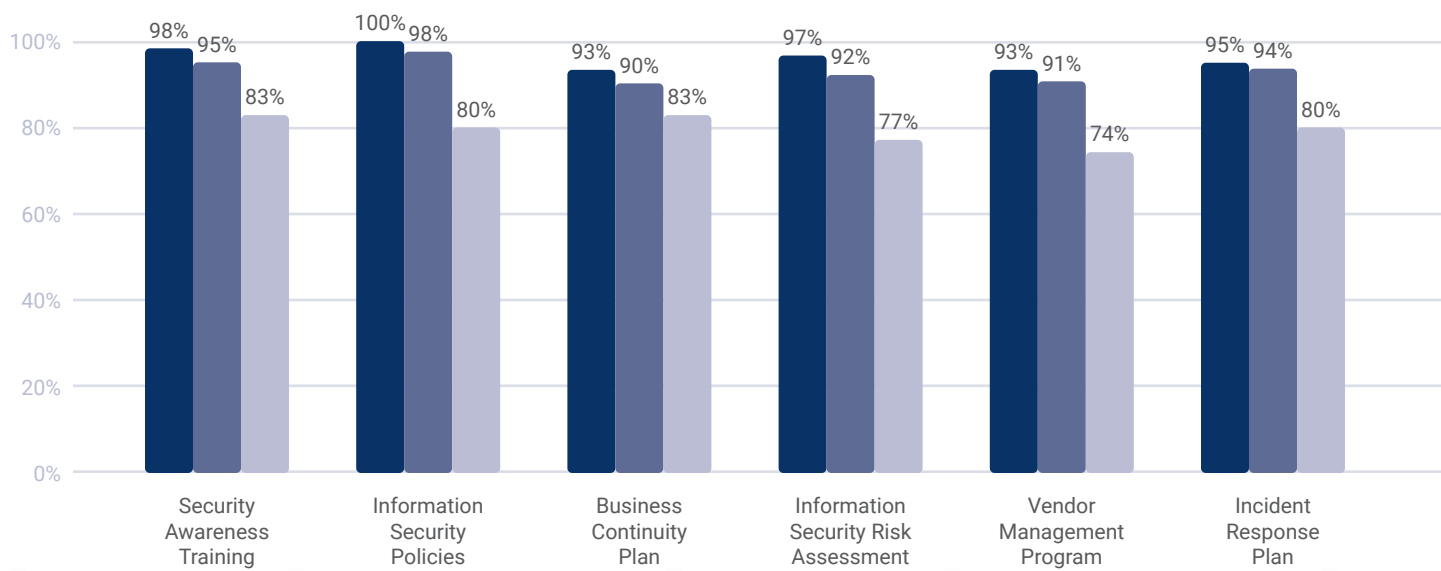
CYBERSECURITY PROGRAM MATURITY



Tuning In

Institutions that report a strong cybersecurity culture are also more likely to report a mature cybersecurity program. Across every program area evaluated, respondents from institutions with a strong culture were more likely to rate their program as at least somewhat mature than those from institutions with developing cultures. Some of the largest differences were observed in risk assessments (97% vs. 77%), policies (100% vs. 80%), vendor management (93% vs. 74%), and incident response (95% vs. 80%).

PROGRAMS RATED AT LEAST SOMEWHAT MATURE BY CULTURE



Takeaway

As a GRC software company, we recognize that we bring a particular perspective to this topic. However, the results align with what we've seen for years:

Managing a cybersecurity program through spreadsheets, folders, and email can work for a while, but it becomes much more difficult as programs mature.

Dedicated GRC tools provide capabilities that are difficult to replicate with shared network locations alone, including structured data, role-based access controls, automated notifications, instant reporting, integrations, and access to security and compliance expertise. These capabilities help institutions organize information, show progress, and communicate results more effectively.

As cybersecurity program components mature, the processes and tools used to manage them need to mature, as well.

TANDEM GRC SOFTWARE

Mature programs need mature tools.

Tandem helps financial institutions replace spreadsheets, shared folders, and disconnected tools with software designed specifically for cybersecurity governance, risk management, and compliance.

Manage assessments, policies, vendors, incidents, business continuity, and more from a single platform built by cybersecurity experts.

[Tandem.App/Demo](https://tandem.app/demo) >



See what your cybersecurity program can look like with Tandem.



Security Awareness Training

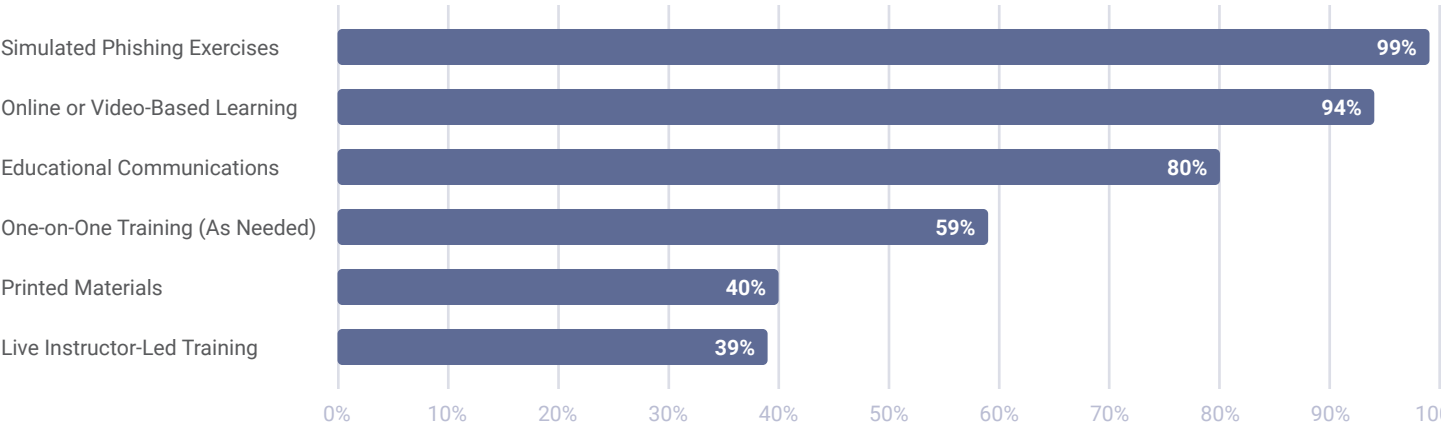
Effective security awareness training programs involve educating employees to identify cybersecurity risks and make informed security decisions in their daily work. Among all program components measured in the survey, security awareness training received the highest maturity ratings. To better understand what highly mature programs look like in practice, we looked at training effectiveness, delivery formats, topics covered, target audiences, and training cadence.

Observation

Strong security awareness programs rely on multiple training methods.

Respondents reported using an average of more than three different training formats, with simulated phishing (99%), online learning (94%), and educational communications (80%) being the most common.

TRAINING METHODS

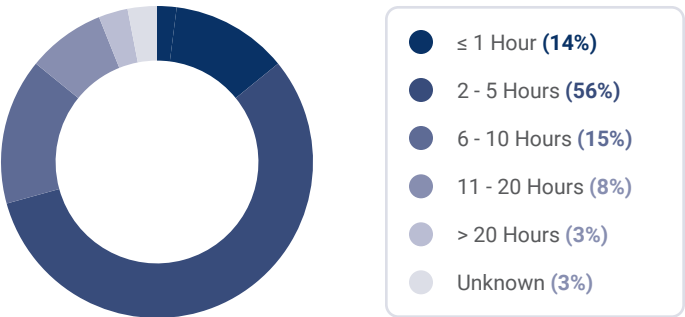


Observation

Two to five hours of annual training is most common.

A majority of respondents (56%) reported requiring between two and five hours of security awareness training annually, making it the most common approach by a significant margin.

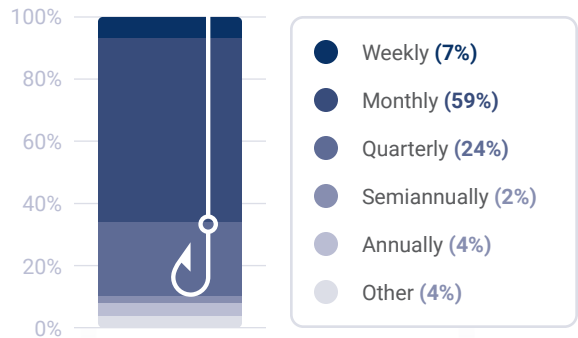
TIME SPENT ON TRAINING



Tuning In

Among institutions that conduct simulated phishing exercises, monthly testing emerged as the standard cadence (59%). Nine in ten respondents reported performing phishing tests on at least a quarterly basis.

PHISHING TEST FREQUENCY

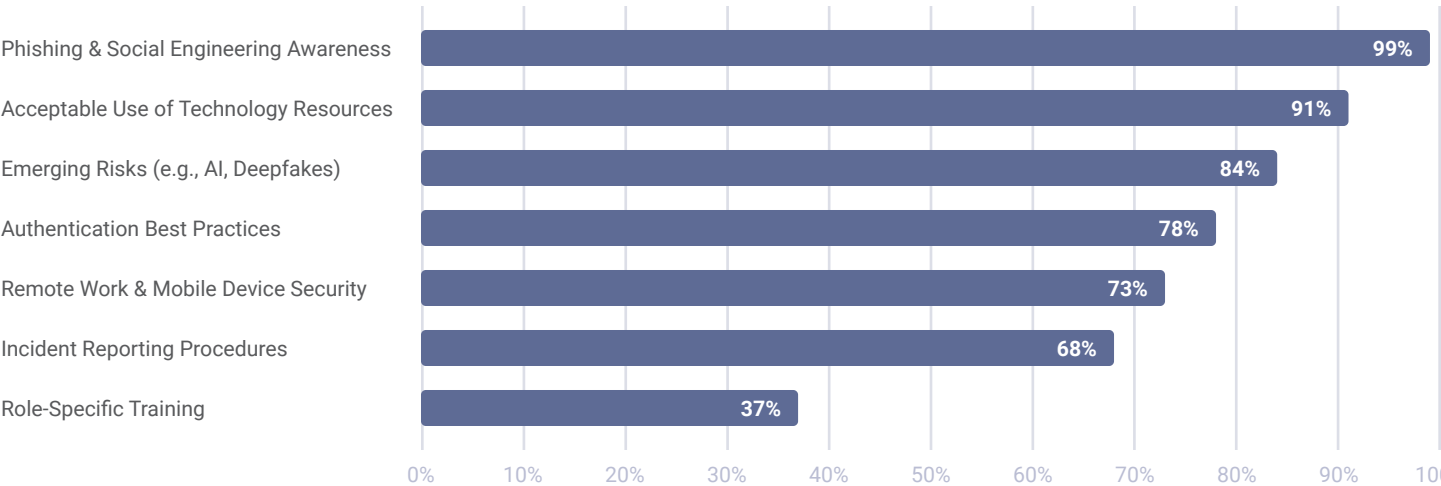


Observation

Emerging threats have become mainstream training content.

While phishing and social engineering remain nearly universal training topics (99%), a large majority of institutions also include emerging risks such as artificial intelligence and deepfakes (84%). Notably, emerging risks were covered more frequently than remote work security (73%), incident reporting procedures (68%), and role-specific training (37%).

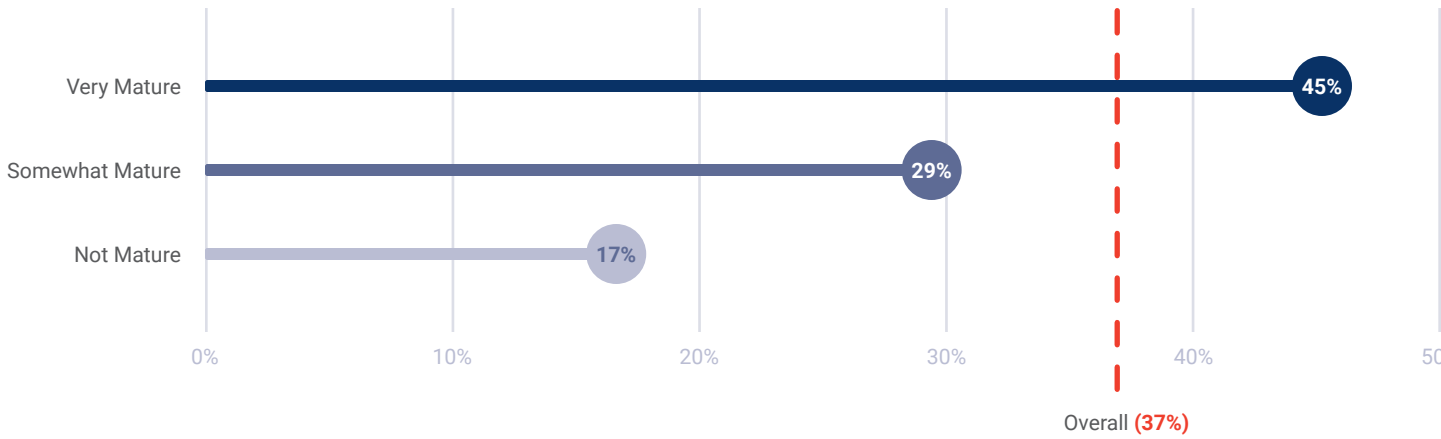
TRAINING TOPICS



Tuning In

While role specific training was reported by only 37% of respondents, it was more common among institutions with mature training programs. Approximately 45% of respondents rating their training “very mature” included role-specific content, compared with 29% of those rating it “somewhat mature.”

ROLE-SPECIFIC TRAINING BY PROGRAM MATURITY

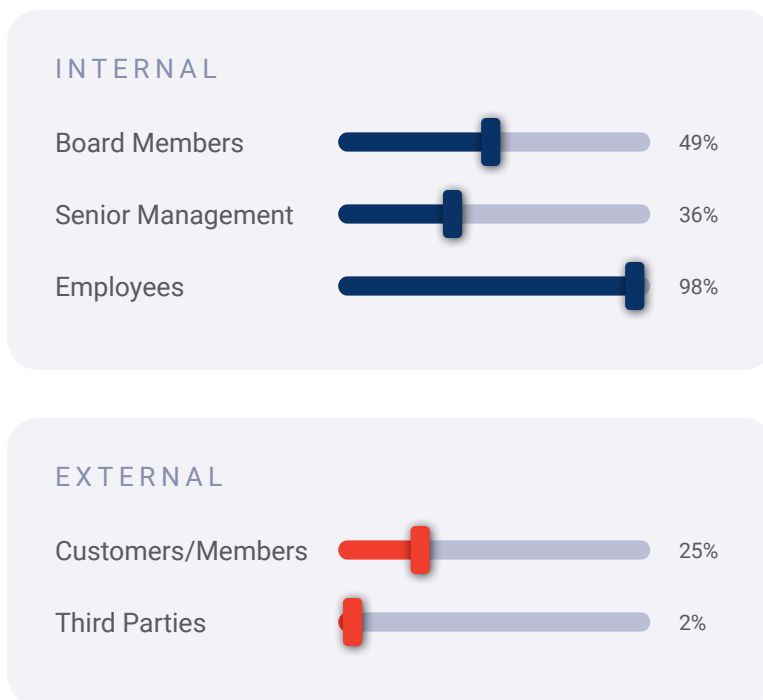


Observation

Training programs prioritize the workforce.

Security awareness training is nearly universal among employees, with 98% of respondents reporting that employees receive training. Many institutions extend training to other internal audiences, including Boards (49%) and senior management (36%), as well as external audiences, like customers or members (25%).

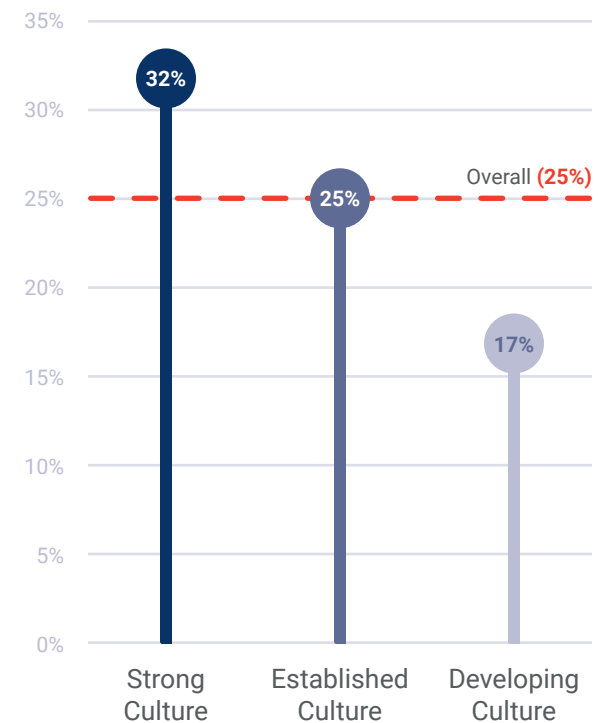
TRAINING AUDIENCES



Tuning In

Institutions that view cybersecurity as part of their culture seem to be more likely to extend that focus beyond the institution. Participation in customer and member cybersecurity education increased from 17% among respondents with developing cultures to 32% among those with strong cultures.

CUSTOMER TRAINING BY CULTURE



Takeaway

Most institutions report having a well-established security awareness training program, and survey data suggests these efforts tend to mature alongside cybersecurity culture. Maturity does not necessarily mean “do more training” or “create individualized content for every role.” Instead, the strongest programs focus on the people and activities most closely connected to the institution’s risks.

- **For institutions with established programs**, maturity may come from refining the program, not expanding it. Keep content timely, relatable, and connected to the institution’s cybersecurity risks.
- **For institutions with developing programs**, maturity does not have to happen all at once. Start by identifying your highest-priority risks. Then, select training topics and methods most likely to influence behavior.

At the end of the day, an effective security awareness training program is not defined by how much training is provided, but by whether it helps build a culture where cybersecurity becomes part of how people think and make decisions.

Incident Management

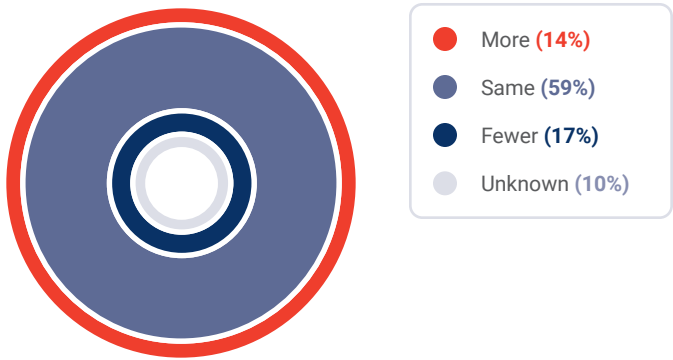
Incident management is the process of detecting, responding to, and recovering from incidents. Among all cybersecurity program components measured in the survey, incident response programs received the *lowest* maturity ratings. To better understand how financial institutions are approaching incident response, we looked at changes in cybersecurity incident volume, experiences with specific types of incidents, and confidence in detecting incidents as they occur.

Observation

Incident volume has remained relatively stable.

Nearly six in ten institutions (59%) reported experiencing the same number of cybersecurity incidents as the previous year. Among the remaining respondents, 14% reported more incidents and 17% reported fewer incidents, indicating no clear shift in overall incident volume.

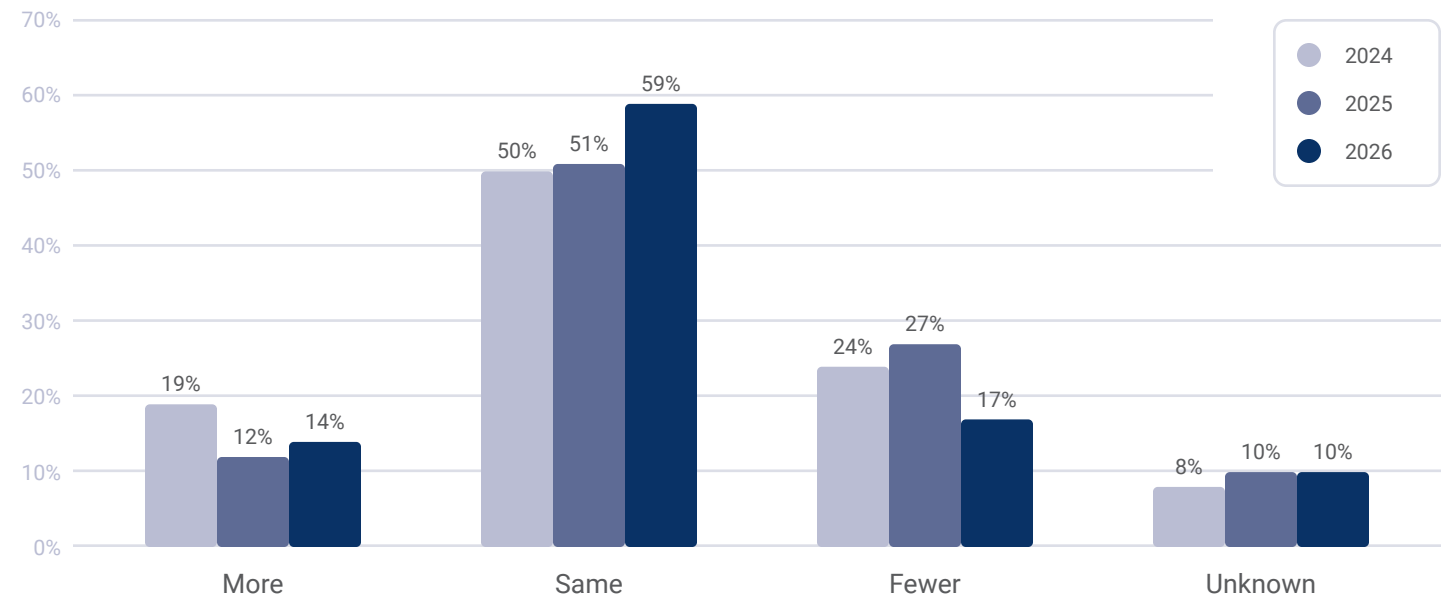
CHANGE IN INCIDENT VOLUME



Tuning In

While most respondents reported no change in 2026, the broader trend suggests cybersecurity incidents remain a consistent reality for financial institutions. Nearly three-quarters of respondents (73%) reported the same or more incidents than the previous year.

YEAR-OVER-YEAR CHANGE IN INCIDENT VOLUME



Observation

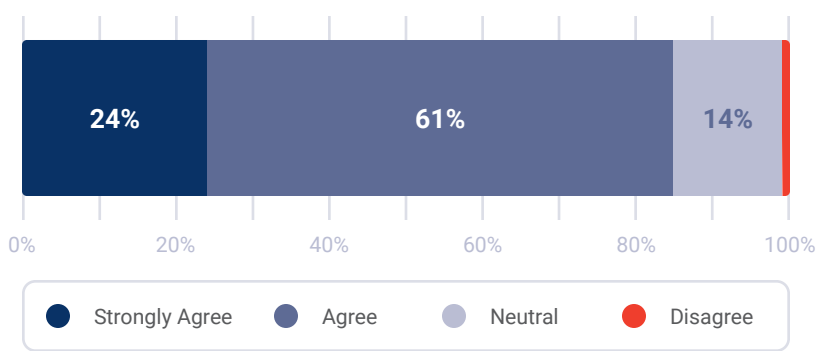
Most believe training lowers incident risk.

Respondents were asked to indicate the extent to which they agreed or disagreed with the following statement:

“My financial institution’s cybersecurity training directly reduces the risk of incidents.”

A significant majority of respondents (85%) agreed or strongly agreed, while only 1% disagreed, suggesting most institutions view training as an effective risk-reduction measure.

TRAINING REDUCES RISK OF INCIDENTS



Tuning In

Nearly all respondents from institutions with a strong cybersecurity culture (97%) and most from institutions with a very mature incident response plan (91%) agreed training reduces risk of cybersecurity incidents.

TRAINING IMPACT BY CULTURE

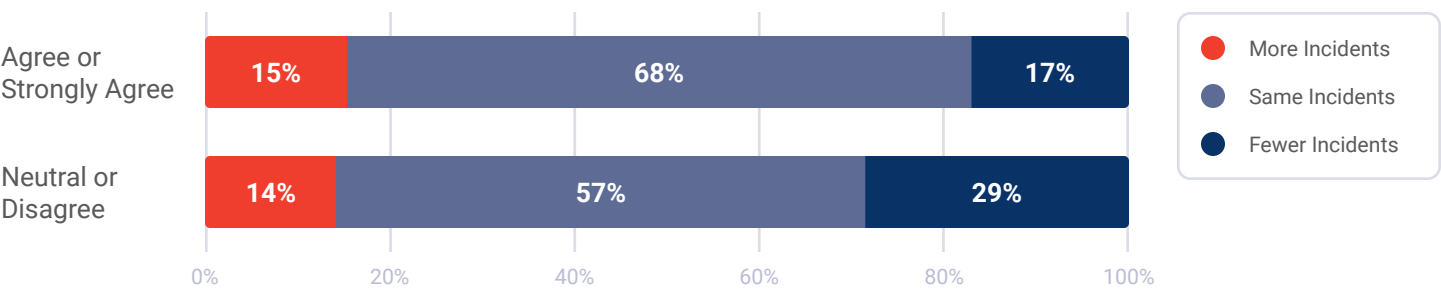


TRAINING IMPACT BY IRP MATURITY



However, this belief was not associated with more favorable incident trends. Institutions that believed training directly reduces risk were just as likely to report an increase in incidents as those that were less convinced (15% vs. 14%). This does not diminish the importance of training, but it does reinforce the need for a layered cybersecurity program.

INCIDENT VOLUME BY TRAINING IMPACT



Observation

Many are confident in incident detection.

Most respondents expressed confidence in their institution’s ability to detect a cybersecurity incident while it is happening. Nearly six in ten (59%) reported being either “very confident” or “extremely confident,” while another 33% reported being “moderately confident.”

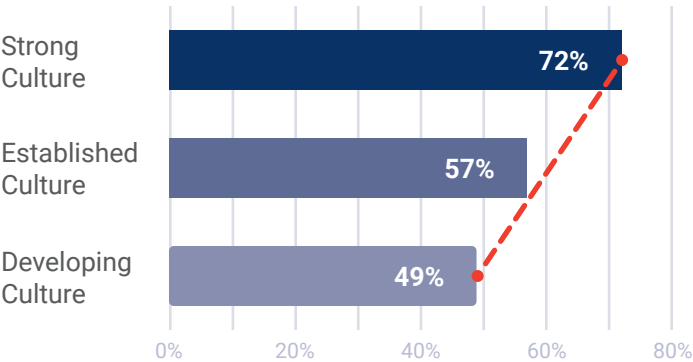
INCIDENT DETECTION CONFIDENCE



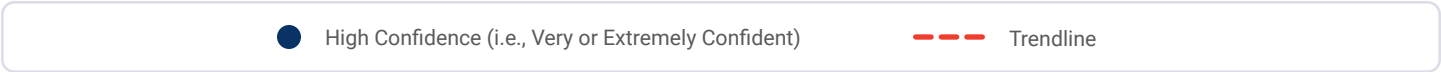
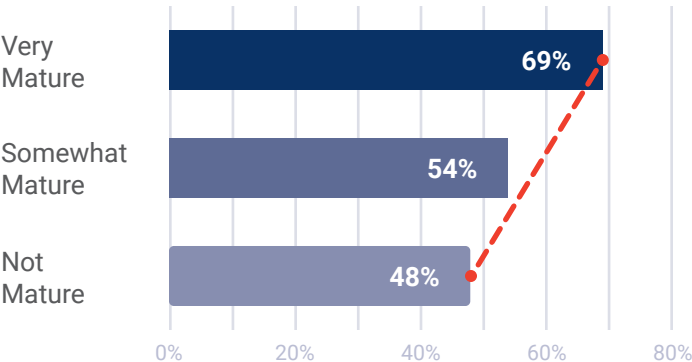
Tuning In

Institutions with stronger cybersecurity cultures and more mature incident response programs were more likely to express high confidence in their ability to detect incidents. High confidence was reported by 72% of respondents with a strong culture, compared with 49% of those with a developing culture. Similarly, respondents with very mature incident response plans (69%) were more likely to express high confidence than those with lower plan maturity (48%).

DETECTION CONFIDENCE BY CULTURE



DETECTION CONFIDENCE BY MATURITY

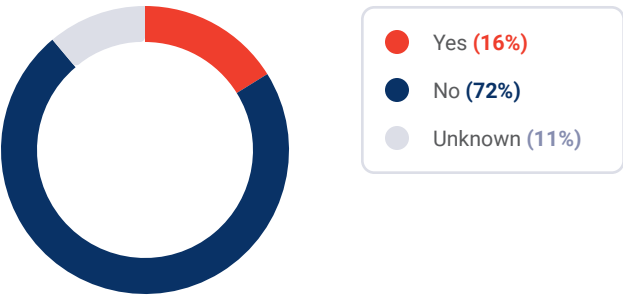


Observation

AI-enabled fraud affected one in six institutions.

Sixteen percent of respondents reported experiencing a fraud incident involving AI-generated or AI-assisted content, such as deepfakes, voice cloning, or synthetic identities, in the past 12 months. While most institutions (72%) reported no such incidents, the results suggest that AI-enabled fraud has become a real-world challenge for many institutions.

ARTIFICIAL INTELLIGENCE INCIDENTS

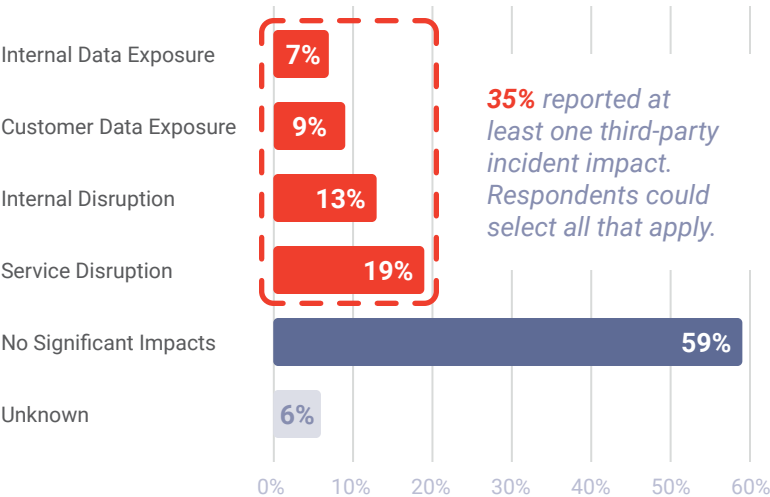


Observation

One in three impacted by third-party incident.

More than one-third of respondents (35%) reported experiencing at least one significant impact from a third-party incident during the past 12 months. The most common outcome was an operational disruption rather than data exposure (i.e., compromise, loss, or exposure of data).

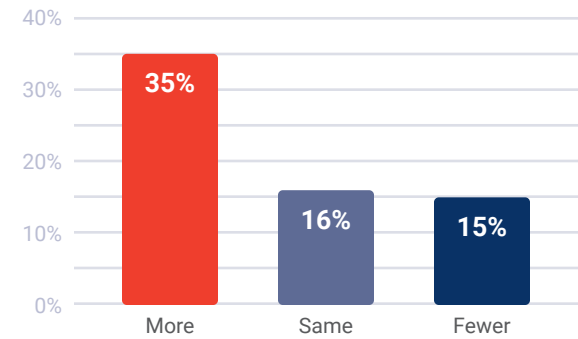
THIRD-PARTY INCIDENT IMPACTS



Tuning In

Institutions reporting higher cybersecurity incident volumes were more likely to report AI-related incidents. Specifically, 35% of respondents reporting more incidents experienced an AI-related incident, compared with about 15% of those reporting stable or declining incident volumes.

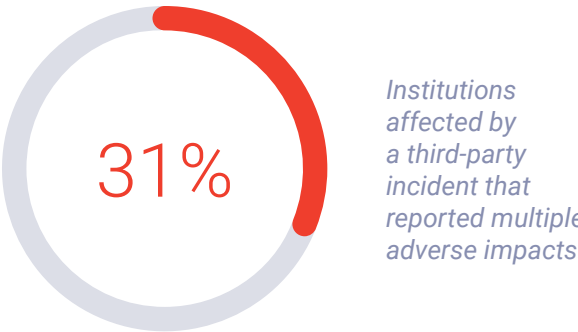
AI INCIDENTS BY VOLUME



Tuning In

When third-party incidents occur, they rarely fit into a single category. Among respondents who reported experiencing significant third-party incident impacts, nearly one-third (31%) reported multiple adverse impacts, with 7% experiencing disruptions to both customer-facing services and internal operations.

MULTIPLE IMPACTS



Takeaway

Of the six cybersecurity program components evaluated, incident response received the fewest “very mature” ratings (33%). Assessing maturity in this area presents a unique challenge. Institutions need a plan, but documentation alone cannot show how well the plan will work under pressure.

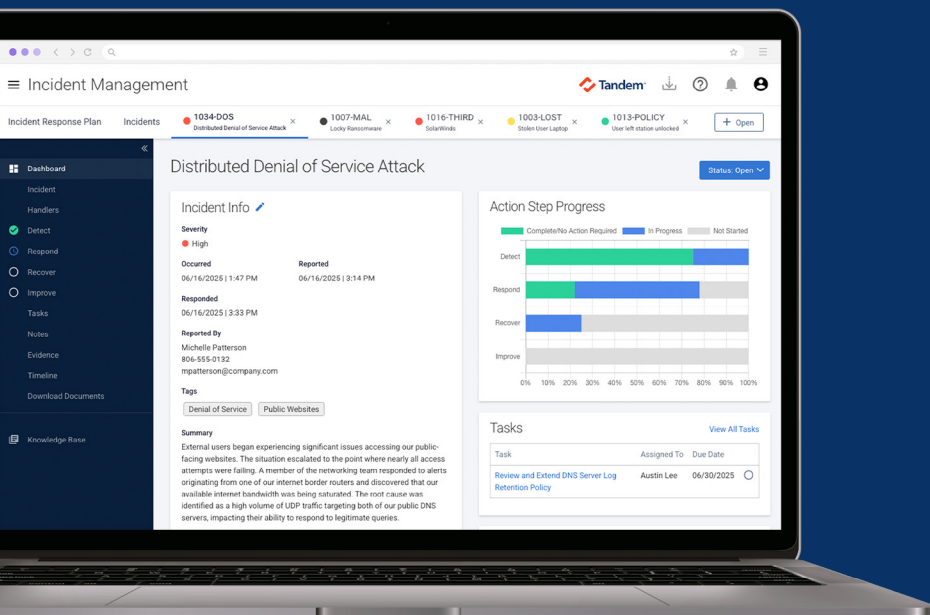
Institutions looking to strengthen their plans should focus on these areas:

- **Test the plan.** Use exercises to rehearse your response activities and validate confidence in detection capabilities, escalation procedures, and decision-making.
- **Prepare for broader impacts.** AI-enabled fraud, third-party disruptions, and other incidents may impact several operational areas at once.
- **Turn experience into improvement.** If an incident occurs, use the opportunity to strengthen procedures, clarify responsibilities, and update employee training.

Each encounter should leave the institution better prepared to limit disruption and respond effectively to future events.

TANDEM INCIDENT MANAGEMENT

Be ready before an incident happens.



Keep incident records organized



Track response actions from start to finish



Use scenarios to host tabletop exercises

[Tandem.App/IM](https://tandem.app/im) >

Prepare to handle incidents with Tandem Incident Management.



Cyber Insurance

Cyber insurance has become a key part of incident management, allowing organizations to transfer a portion of an incident’s financial risk. To better understand the current state of cyber insurance, we looked at whether institutions carry cyber insurance coverage, how premiums have changed, and trends in claim filing.

Observation

Nearly every institution carries cyber insurance.

Nearly all respondents (96%) reported that their institution maintains a cyber insurance policy, while only 1% reported having no coverage.

CYBER INSURANCE COVERAGE

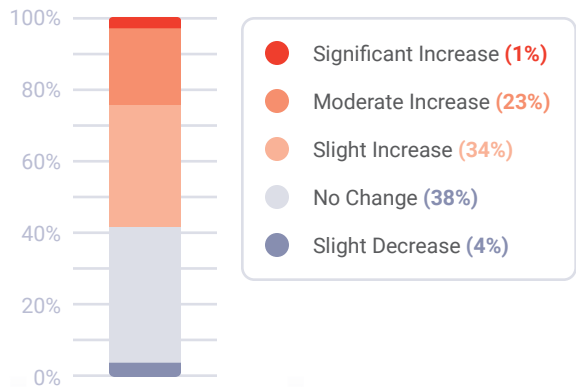


Observation

Cyber insurance costs trend upward.

Among respondents who knew how their premiums changed at the most recent renewal, 58% reported an increase and 38% reported premiums stayed about the same.

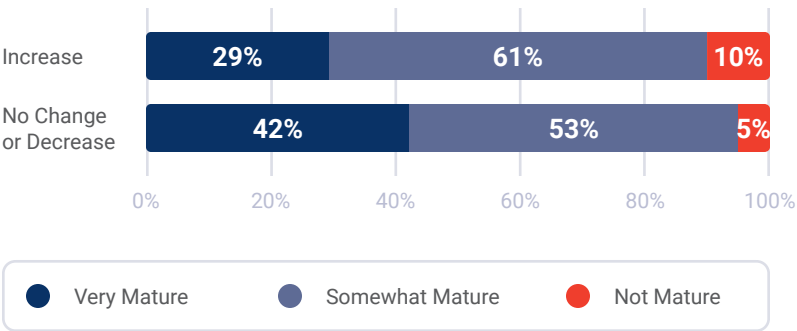
INSURANCE PREMIUM CHANGE



Tuning In

While many factors influence cyber insurance pricing, respondents with stable or declining premiums were more likely to describe their incident response programs as “very mature” than respondents reporting premium increases (42% vs. 29%).

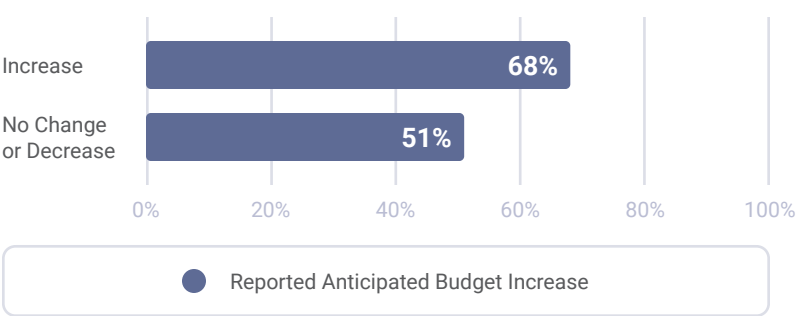
IRP MATURITY BY PREMIUM CHANGE



Tuning In

Respondents who reported an increase in cyber insurance premiums were also more likely to report an increase in their anticipated cybersecurity spending (68% vs. 51%), as a whole. While this relationship does not explain the increase, it does suggest that rising insurance costs are often part of a larger cybersecurity spending picture.

BUDGET GROWTH BY PREMIUM CHANGE



Observation

Few reported filing insurance claims.

Despite near-universal adoption, only 7% of respondents reported filing a claim on their cyber insurance in the past 24 months.

Tuning In

A cybersecurity incident is any event that compromises the confidentiality, integrity, or availability of systems or data. While not every cybersecurity incident is likely to result in an insurance claim, responding to an incident often requires time, effort, and resources from the institution, regardless of whether a claim is filed.

This distinction is evident in the results. Among those who reported experiencing AI-related fraud or third-party incident impacts, 83% did not report filing a claim.

A similar pattern emerged when comparing claim activity to incident volume trends. Even among respondents who reported experiencing more incidents over the past 12 months, only 15% reported filing a claim. Claim rates were even lower among institutions reporting the same number of incidents (6%) or fewer incidents (4%).

Takeaway

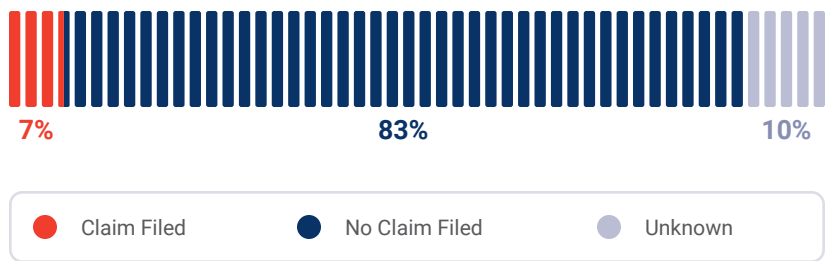
Cyber insurance is now common among financial institutions, but coverage alone does not determine how well an institution can manage the financial impact of a cybersecurity event or incident. The value of a cyber insurance policy depends on whether the institution understands its coverage and knows how to use the policy when an incident occurs.

When evaluating cyber insurance coverage, institutions should consider the following:

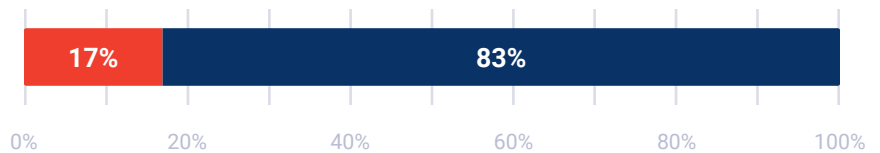
- **Review how the policy fits into the incident response process.** Institutions should know when the carrier must be notified, who is responsible for initiating a claim, and what documentation may be required.
- **Understand the terms before an incident occurs.** Coverage limits, exclusions, deductibles, and requirements to use approved legal counsel or response providers can affect how an institution responds to an incident.
- **Plan for costs or events that may fall outside the policy.** Not every incident results in a claim. Even covered events may involve expenses that are not fully reimbursed. Institutions should be prepared to absorb some costs as part of incident recovery.

Cyber insurance should support a prepared incident response program, not replace one. Institutions that understand their coverage and plan for uninsured costs are likely to be better positioned to handle financial impacts of an incident.

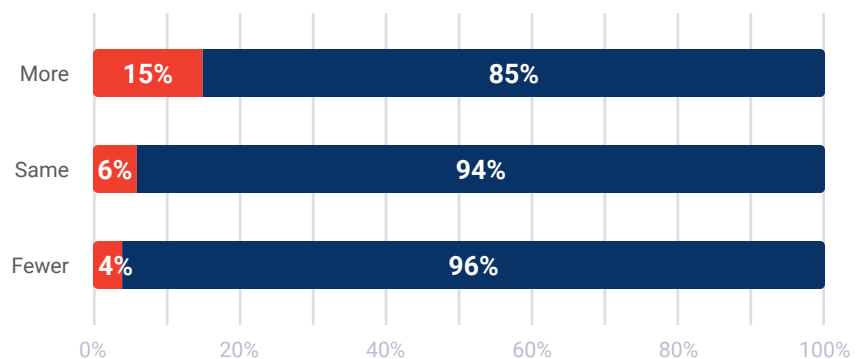
CYBER INSURANCE CLAIM STATUS



CLAIMS BY INCIDENT IMPACT



CLAIMS BY INCIDENT VOLUME



KEYS Conference

April 6 - 8, 2027 | The Overton Hotel | Lubbock, Texas

Knowledge Essential to Your Security

Each spring, Tandem customers gather for three days of learning, connection, and collaboration designed to help IT and information security professionals stay current, share experiences, and strengthen their programs with real-world insights.



EXPERT INSIGHT

Hear from industry leaders, Tandem experts, and your peers.



HANDS-ON LEARNING

Build practical skills through educational sessions and workshops.



FOCUSED CONTENT

Explore the latest in cybersecurity governance, risk management, and compliance.



FUN & GAMES

Compete, connect, and enjoy friendly challenges throughout the event.

Learn More & Register Now

[Tandem.App/KEYS >](#)

Tune in to cybersecurity at the 2027 KEYS Conference.



Vendor Management

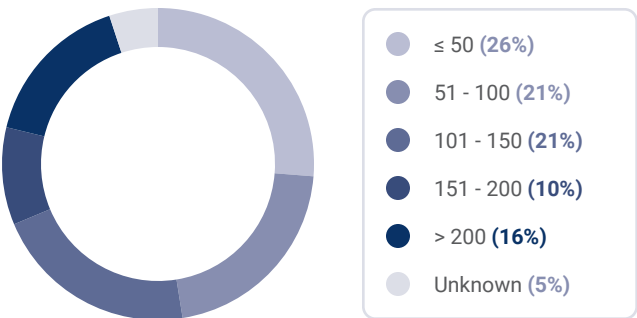
Vendor management is the process of overseeing third-party relationship risk throughout the vendor lifecycle. Among all cybersecurity program components measured in the survey, vendor management was also one of the lowest rated in terms of reported maturity. To better understand current practices, we looked at the number of vendors institutions manage, monitoring cadence, and evaluated third-party artificial intelligence (AI) risk.

Observation

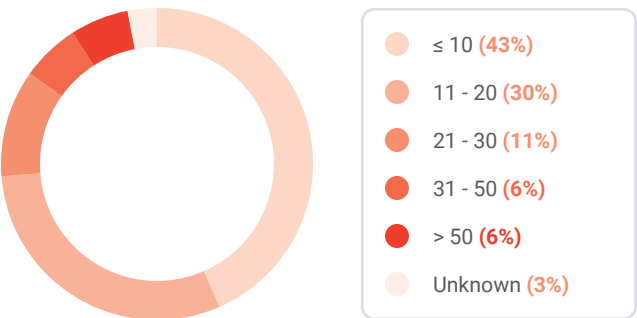
Managing large vendor populations is the norm.

Financial institutions often manage a substantial number of third-party relationships. Nearly half of all respondents (47%) reported maintaining over 100 vendors, including 16% with more than 200 vendors. Even so, 73% of all respondents reported 20 or fewer critical vendors.

NUMBER OF VENDORS



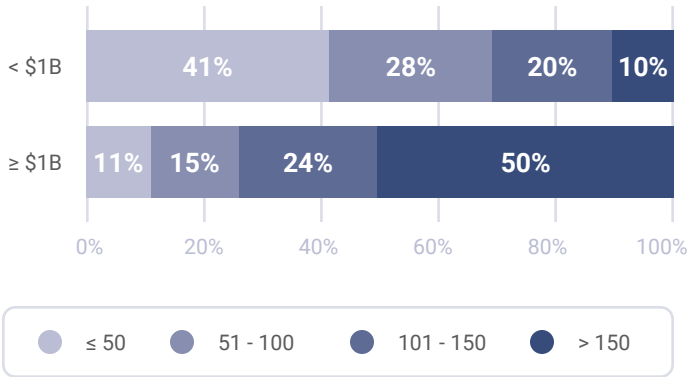
NUMBER OF CRITICAL VENDORS



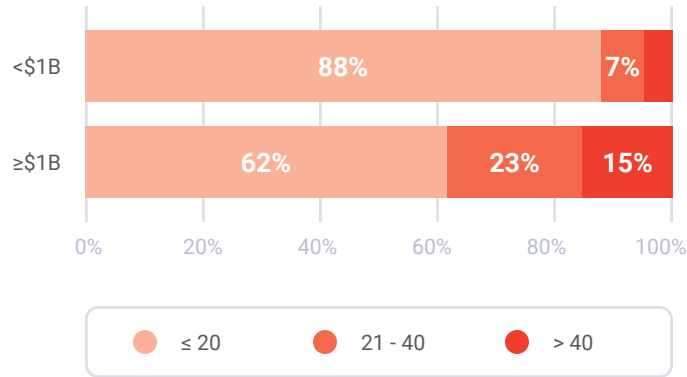
Tuning In

Institution size often influences the scale of a vendor management program. Among institutions with less than \$1 billion in assets, 41% managed 50 or fewer vendors, while only 10% managed more than 150. In contrast, half (50%) of institutions with \$1 billion or more in assets reported more than 150 vendors. Similarly, 88% of smaller institutions reported 20 or fewer critical vendors, compared to 62% of larger institutions.

TOTAL VENDORS BY ASSET SIZE



CRITICAL VENDORS BY ASSET SIZE

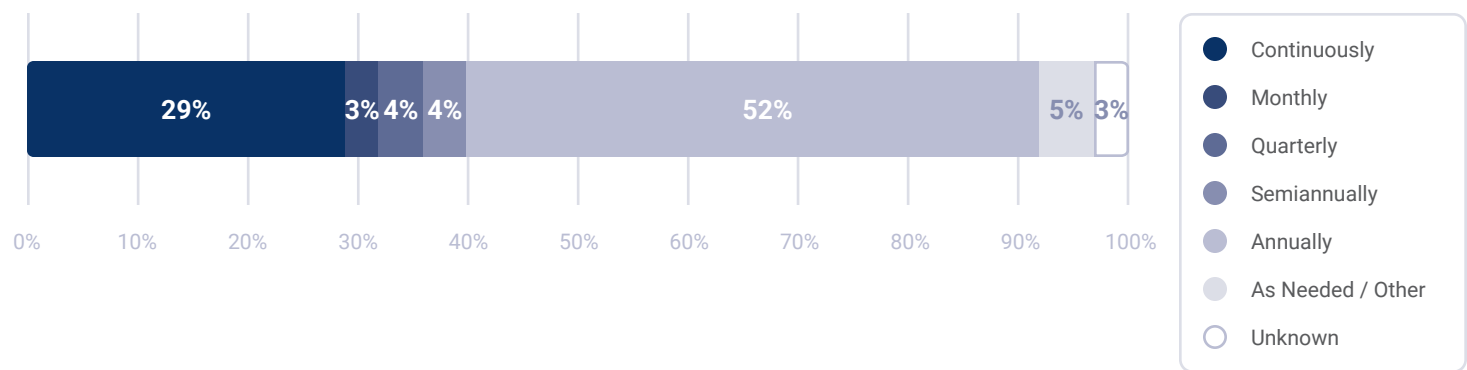


Observation

Monitoring practices tend to follow two distinct approaches.

Vendor monitoring practices tended to group around two primary approaches: annual reviews (52%) and continuous monitoring (29%). All other monitoring frequencies combined accounted for less than one-fifth of responses.

VENDOR MONITORING PRACTICES

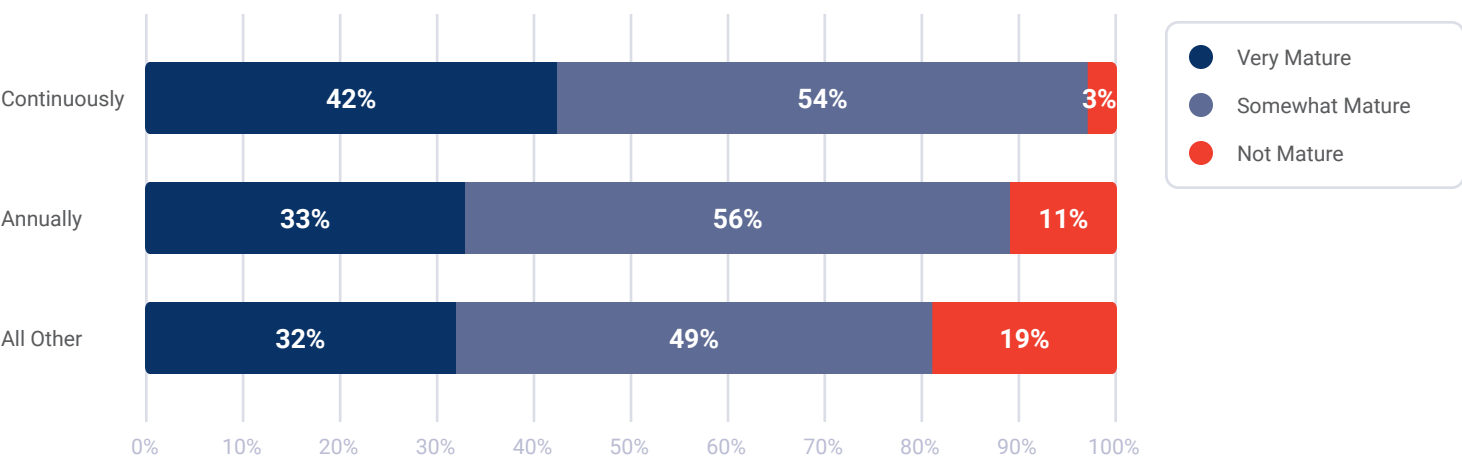


Tuning In

An observable relationship exists between vendor monitoring frequency and perceived program maturity. Institutions conducting continuous monitoring reported the highest percentage of very mature vendor management programs (42%) and the lowest percentage of not mature programs (3%).

Annual monitoring followed closely, with 33% reporting very mature programs and 11% reporting not mature programs. By comparison, institutions using other monitoring frequencies reported not mature programs nearly twice as often as those conducting annual reviews.

PROGRAM MATURITY BY MONITORING FREQUENCY



Need help monitoring your vendors?
Connect with a Tandem partner.

Tandem.App/Partner-Program ➤

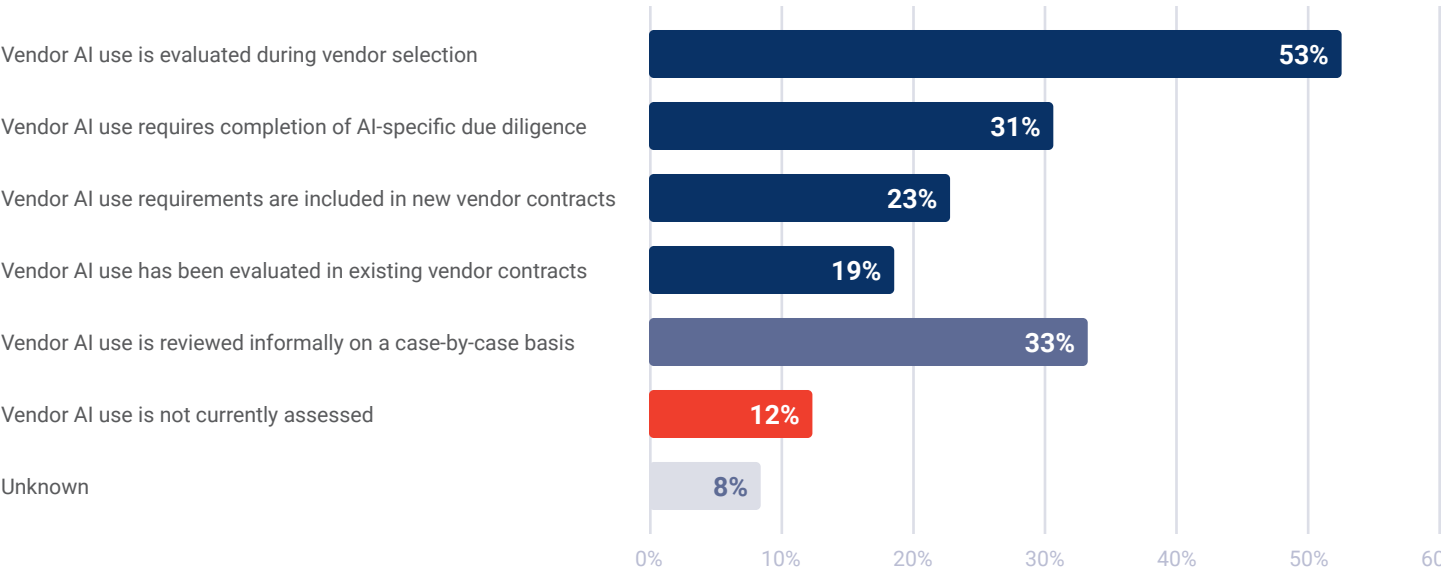
Observation

Vendor AI oversight practices remain uneven.

Many institutions are still developing their approach to vendor artificial intelligence (AI) governance. More than half of respondents (53%) reported evaluating vendor AI use during vendor selection, making it the most common vendor AI oversight practice.

No other AI oversight activity was reported by more than one-third of respondents. At the same time, 33% reported reviewing vendor AI use informally on a case-by-case basis, and 12% reported that vendor AI use is not currently assessed.

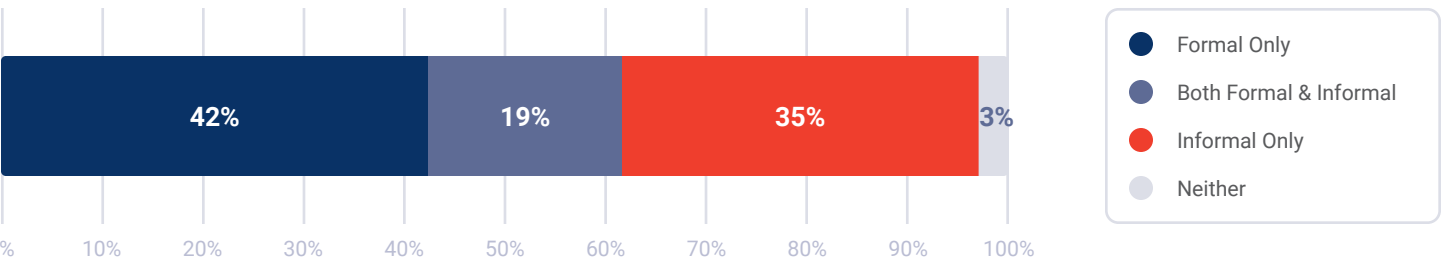
VENDOR AI OVERSIGHT PRACTICES



Tuning In

Sixty-one percent of respondents reported at least one formal process for evaluating vendor AI use. At the same time, 19% selected both formal and informal responses, indicating that vendor AI governance practices may vary across vendors, use cases, or stages of the relationship lifecycle. Only 42% reported exclusively formal approaches, while 38% reported only informal, nonexistent, or unknown vendor AI oversight practices.

VENDOR AI OVERSIGHT FORMALITY



Takeaway

Many institutions manage a large number of vendor relationships, but not every vendor requires the same level of oversight. The challenge is in making sure the right oversight happens at the right time.

To increase the maturity of your vendor management program:

- **Establish a consistent cadence.** Ad hoc processes make it easier for important tasks to fall through the cracks. Schedule due diligence, contract reviews, and monitoring activities on a regular basis or use available tools to perform continuous monitoring.
- **Perform due diligence with a purpose.** Rather than treating every vendor the same, focus your due diligence efforts on the nature of the services they provide, the system and data they can access, and the risks they introduce.
- **Make AI part of the conversation.** As vendors continue to incorporate AI into their products and services, it is important for vendor managers to include questions about AI use within existing selection, due diligence, contract review, and monitoring processes.

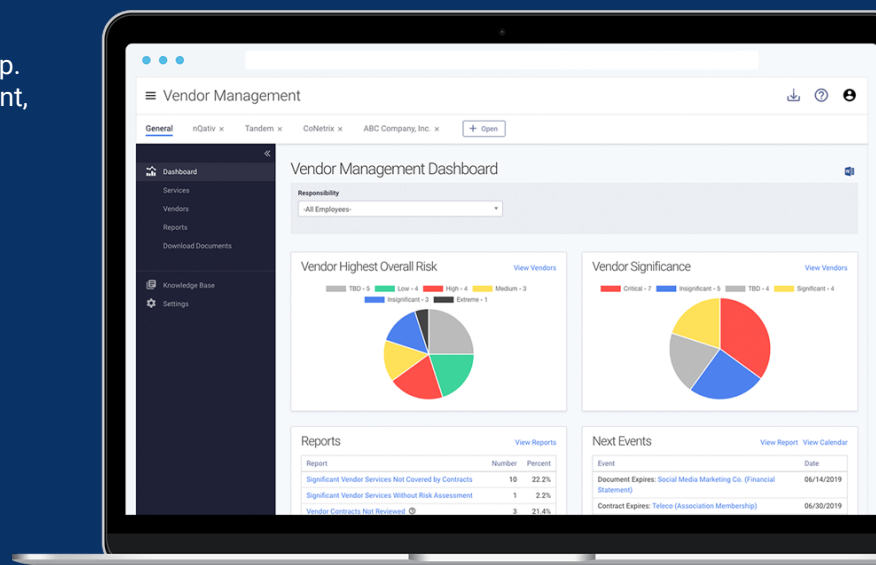
Vendor management is ultimately an ongoing process, not a point-in-time exercise. Regular reviews and meaningful due diligence help institutions stay informed as vendors, services, and technologies change.

TANDEM VENDOR MANAGEMENT

Manage third-party risk with confidence.

Tandem Vendor Management helps organizations manage third-party risk throughout the entire relationship. From planning and due diligence to contract management, ongoing monitoring, and termination, Tandem keeps information, documents, reviews, and reporting organized in one place.

Tandem.App/VM >



Simplify third-party oversight with Tandem Vendor Management.



Artificial Intelligence

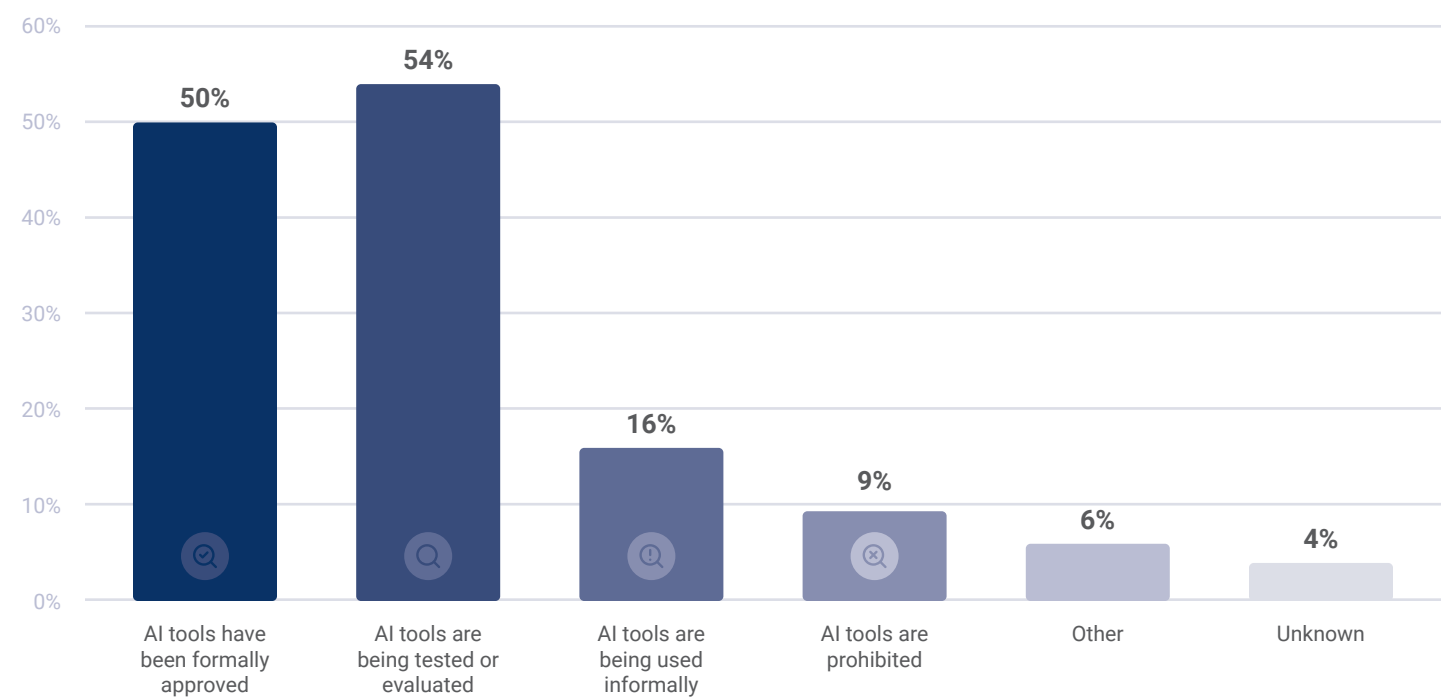
Artificial intelligence (AI) is an emerging cybersecurity risk that financial institutions are actively working to manage. To better understand current practices, we looked at AI adoption rates, the most popular AI tools, unapproved AI usage, and the common concerns institutions have about the use of AI.

Observation

Half of institutions have formally adopted AI.

Half of respondents (50%) reported AI tools have been formally approved for use by their institution, and 54% reported actively testing or evaluating AI tools. Despite this progress, governance challenges remain, with 16% of respondents reporting informal AI use by employees without formal approval or oversight.

AI USE IN FINANCIAL INSTITUTIONS

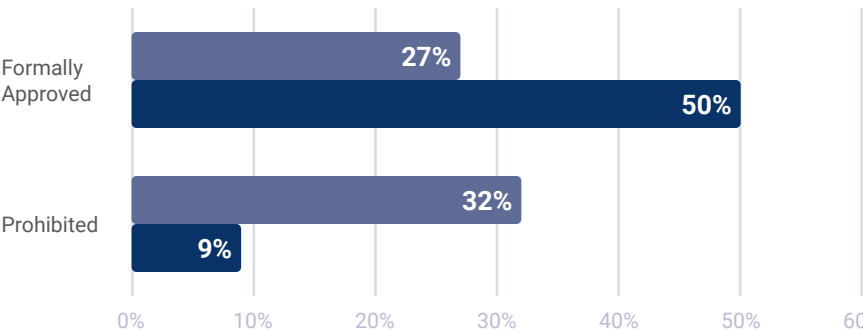


Tuning In

Survey results show a notable shift in AI adoption over the past year. Institutions reporting formally approved AI use increased from 27% in 2025 to 50% in 2026, while the percentage prohibiting AI decreased from 32% to 9%.



YEAR-OVER-YEAR AI POSTURE

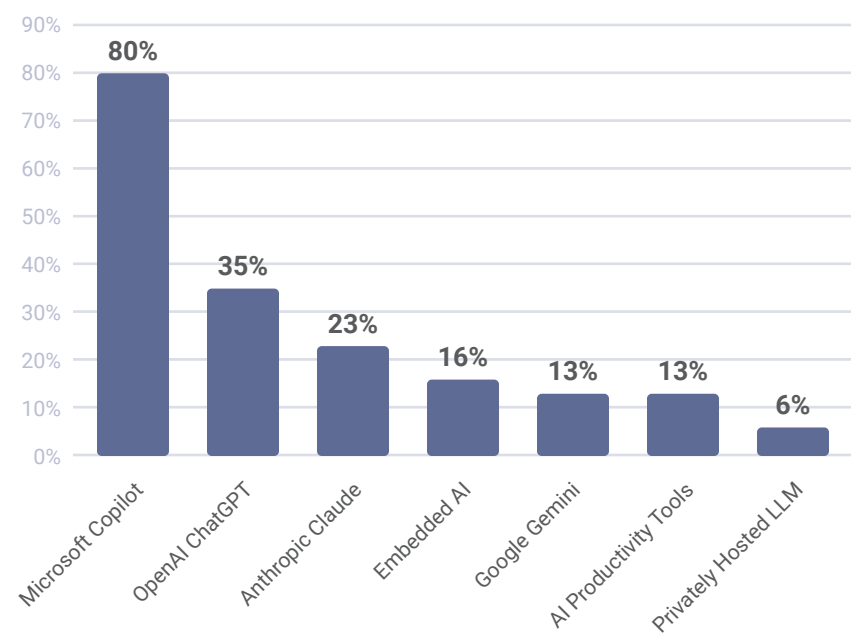


Observation

Microsoft Copilot leads AI tool adoption.

Microsoft Copilot was by far the most widely adopted AI tool, with four in five respondents (80%) reporting that it is being formally used, tested, or evaluated. OpenAI ChatGPT ranked a distant second at 35%, followed by Anthropic Claude at 23%. Adoption levels for other AI tools were substantially lower.

AI TOOL ADOPTION RATES

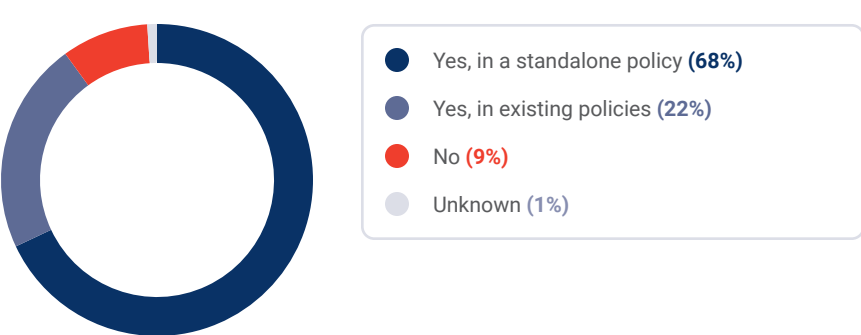


Observation

Approved AI policies are now common.

The vast majority of respondents (90%) reported having an approved AI policy, including 68% with a standalone AI policy and 22% that address AI within existing policies.

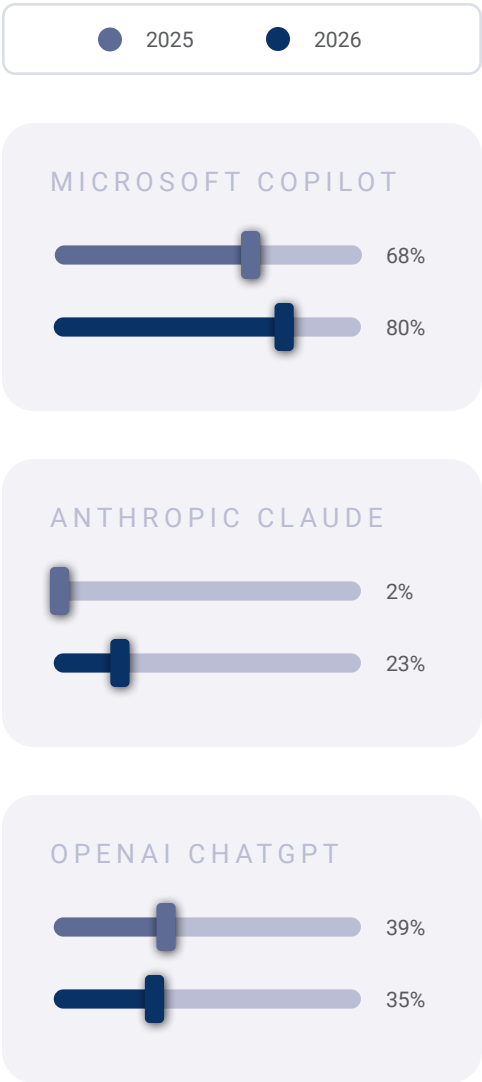
APPROVED AI POLICY



Tuning In

Microsoft Copilot’s lead continued to grow (68% to 80%), while Claude recorded the largest year-over-year increase (2% to 23%). ChatGPT remained widely used, though reported adoption declined slightly (39% to 35%).

YEAR-OVER-YEAR ADOPTION

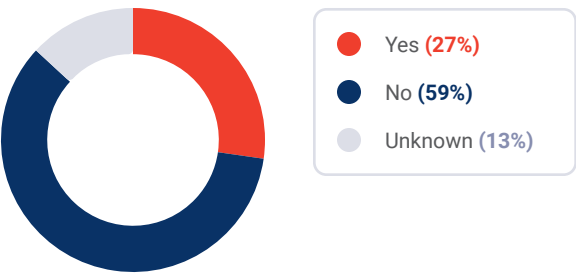


Observation

One in four institutions report shadow AI use.

More than one-quarter of respondents (27%) reported discovering employees using AI tools in unapproved ways during the past 12 months. While a majority (59%) reported no known incidents of unapproved AI use, an additional 13% were unsure.

SHADOW AI DISCOVERY

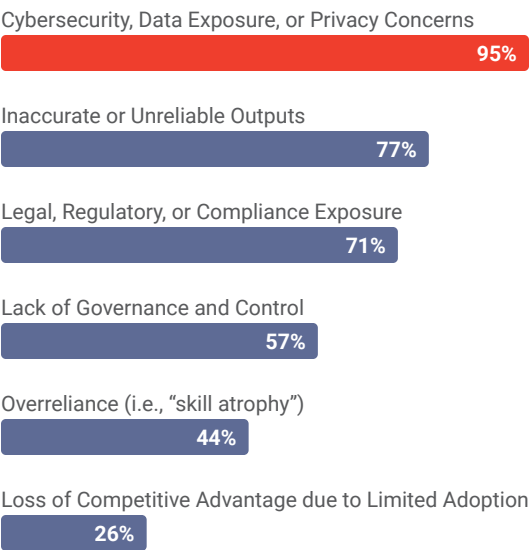


Observation

Cybersecurity risks top the list of AI concerns.

Ninety-five percent of respondents reported concerns about cybersecurity, data exposure, and privacy. Concerns about inaccurate or unreliable outputs (77%) and legal, regulatory, or compliance exposure (71%) were also common.

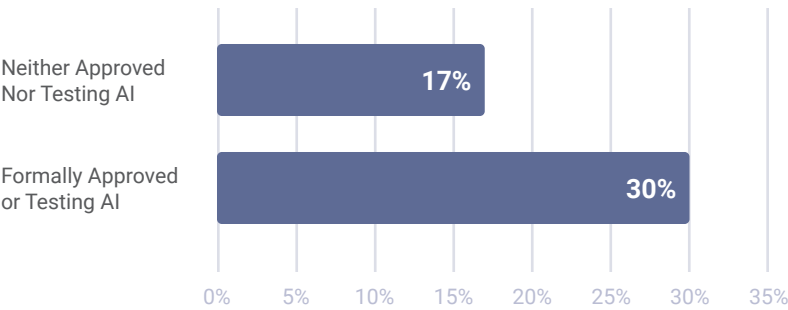
TOP CONCERNS ABOUT AI USE



Tuning In

At first glance, this result may seem counterintuitive, but unapproved AI use was reported *more* frequently by institutions that have adopted or are evaluating AI. Among institutions with approved or tested AI tools, 30% reported discovering shadow AI, compared to 17% of institutions that had neither approved nor tested AI. The difference may reflect higher levels of AI usage, greater awareness of AI-related risks, or increased visibility into how employees are using AI tools.

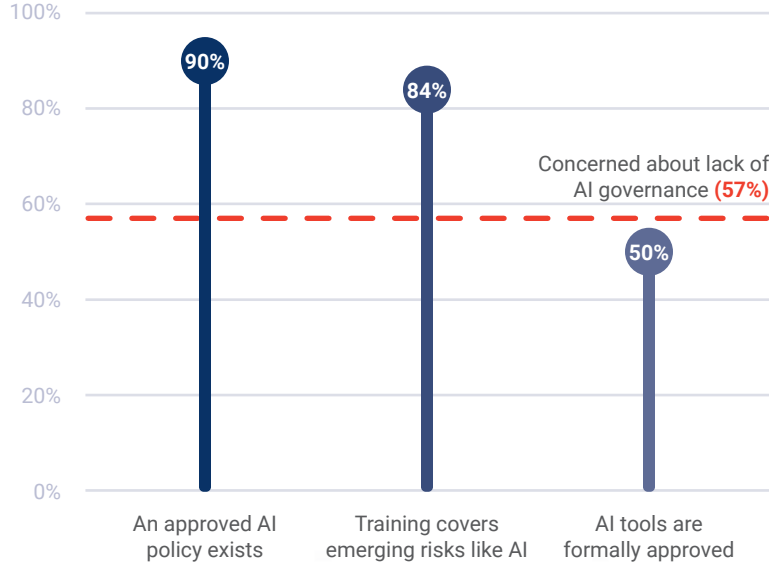
SHADOW AI DISCOVERY BY AI POSTURE



Tuning In

AI governance remains a work in progress, even among institutions with formal programs. Ninety percent of respondents reported having an AI policy, 84% provide training on emerging risks such as AI, and 50% report having formally approved AI tools for use. Despite these oversight and risk management efforts, 57% of respondents still cited a lack of AI governance and control as a concern.

AI GOVERNANCE ACTIVITIES AND CONCERNS



Takeaway

AI adoption and use continue to grow rapidly. Survey results suggest many institutions have moved beyond deciding whether to allow AI and are now focused on managing how it is used. Institutions report some of their greatest concerns with AI involve cybersecurity, governance, and oversight.

Rather than starting from scratch, an institution's existing cybersecurity program can provide a practical starting point for addressing many of these concerns.

- **Vendor management program.** Evaluate, approve, and monitor AI vendors just like any other service provider.
- **Incident response plan.** Ensure your plan addresses how the institution would respond to incidents involving unauthorized disclosure or unapproved use of AI systems.
- **Security awareness training.** Employees should understand which AI tools are approved, what information can be entered into those tools, which use cases are acceptable, and how to request new tools or use cases.

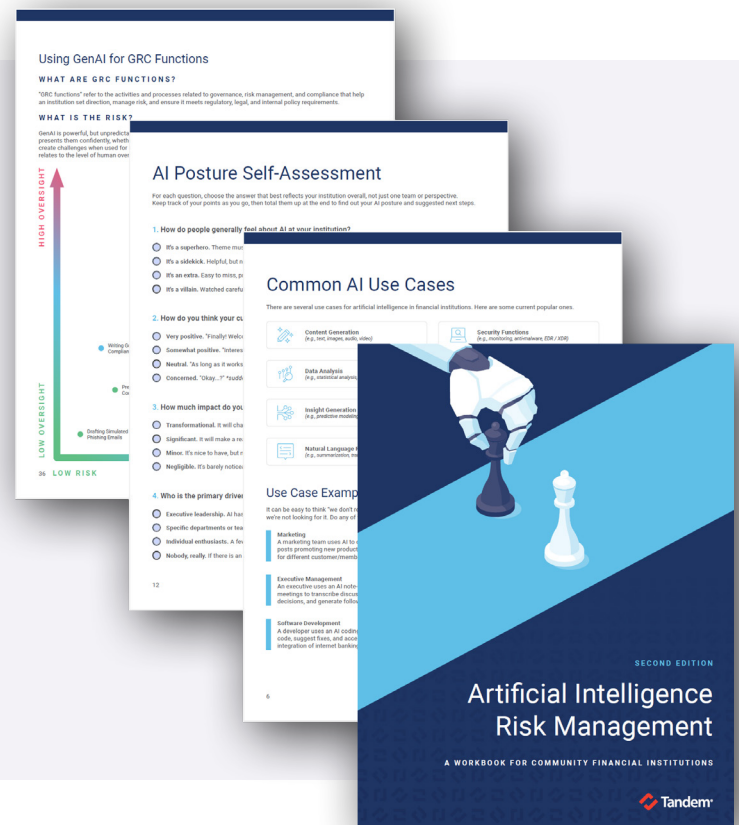
For many institutions, the first step in managing AI risk is not about creating entirely new programs and processes. Instead, focus on improving existing programs, ensuring they are ready for these emerging risks.

Artificial Intelligence Resource

AI is transforming how financial institutions operate, and with new capabilities come new risks. Tandem's *Artificial Intelligence Risk Management Workbook* is designed to help institutions navigate those risks and use AI responsibly.

The workbook includes educational content and interactive worksheets on AI risk assessments, policies, vendor management, employee training, incidents, monitoring and reporting, and more. Use the checkboxes and text fields to answer a series of questions. Then, use the information you learn to help you make informed decisions about AI.

Download the Workbook: Tandem.App/AI-Resources



Compliance

Compliance is how an institution aligns its cybersecurity program with regulatory expectations and established frameworks. Looking at trends in framework adoption, examiner priorities, and compliance monitoring provides some of the clearest signals about an institution’s preparedness for navigating the ever-changing regulatory landscape.

Cybersecurity Assessments

Cybersecurity assessments help financial institutions benchmark the effectiveness of their cybersecurity program against industry standards and frameworks. To better understand current practices, we looked at the most common frameworks used and how their use has changed over time.

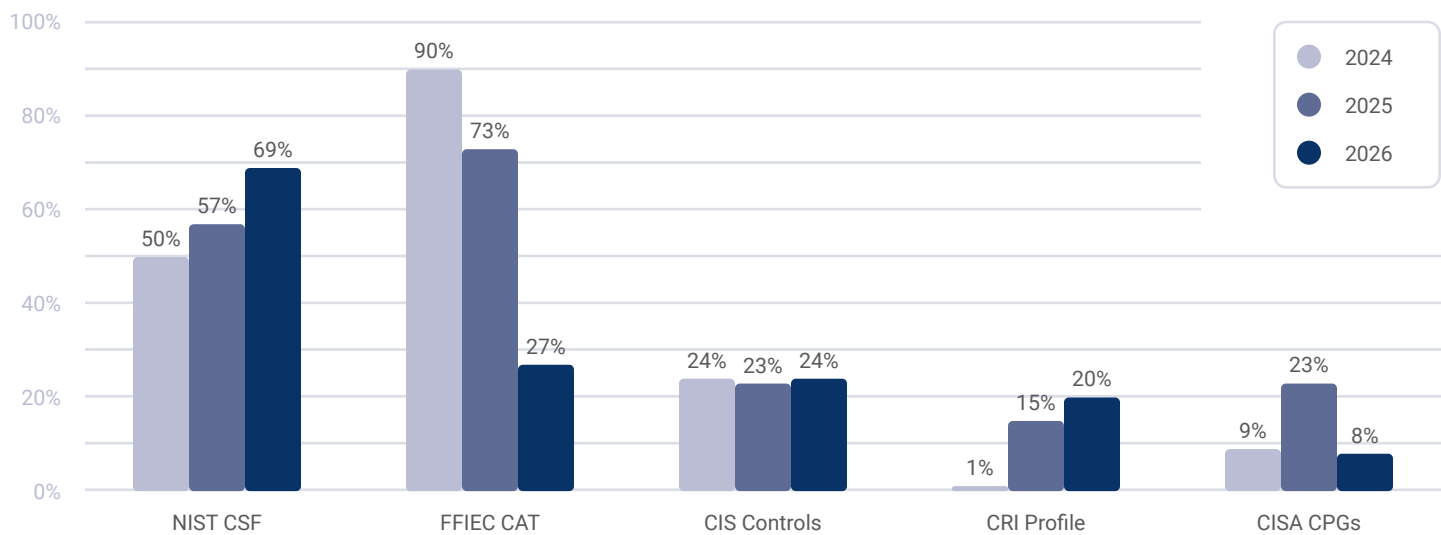
Observation

The NIST CSF is now the most used cybersecurity framework.

More than two-thirds of financial institutions (69%) reported using the NIST Cybersecurity Framework (CSF) in their cybersecurity assessments. Other commonly used frameworks included the CIS Controls (24%) and the Cyber Risk Institute (CRI) Profile (20%). Despite last year’s growth, adoption of the CISA CPGs returned to a lower level this year (8%).

Although the FFIEC Cybersecurity Assessment Tool (CAT) was sunset in August 2025, more than one in four respondents (27%) reported it remains part of their assessment process, underscoring its continued influence within the industry. However, only a very small percent of respondents (3%) reported the FFIEC CAT as their only framework in use.

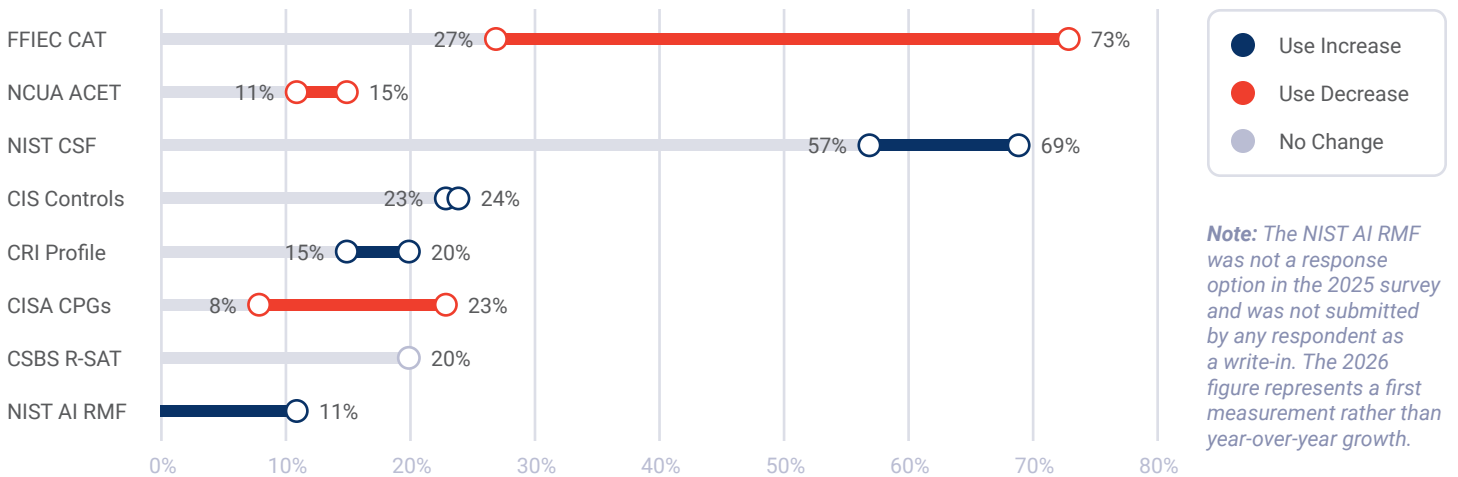
CYBERSECURITY FRAMEWORK USE



Tuning In

Framework use shifted considerably over the past year. Reported use of the FFIEC CAT, NCUA Automated Cybersecurity Evaluation Toolbox (ACET), and CISA Cybersecurity Performance Goals (CPGs) saw a decrease in use. At the same time, the other three frameworks mentioned in the FFIEC CAT Sunset Statement all increased in adoption.

CHANGE IN FRAMEWORK ADOPTION



Observation

Most institutions use more than one framework.

While 39% of respondents reported using one framework, 61% reported using two or more frameworks, and more than a third (37%) reported using three or more frameworks in concert.

Takeaway

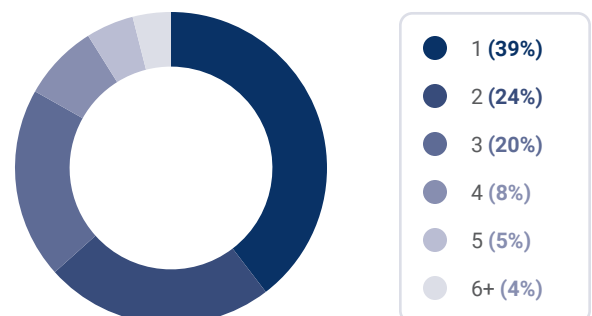
The FFIEC CAT sunset did not result in a one-for-one transition to a new industry standard. While the NIST CSF has emerged as the most widely used framework, institutions have adopted a variety of approaches for performing cybersecurity control self-assessments.

If your institution is currently evaluating or has recently selected a new cybersecurity framework:

- **Ensure the framework fits your institution's size, complexity, and risk.** The best framework is one your institution can consistently use to measure progress and support decision-making.
- **Prepare for changes in Board reporting.** Help your stakeholders understand what is changing, what is not, and how the institution's cybersecurity posture will be communicated with the new framework.
- **Build on the work you've already done.** Many frameworks include mappings to the FFIEC CAT. These mappings can show how existing controls relate to new frameworks, making it easier to explain your transition to stakeholders.

Regulations, threats, technologies, and cybersecurity practices will continue to evolve. Choose a framework that provides meaningful insight today and can evolve with your organization's needs over time.

NUMBER OF FRAMEWORKS USED



Examination Priorities

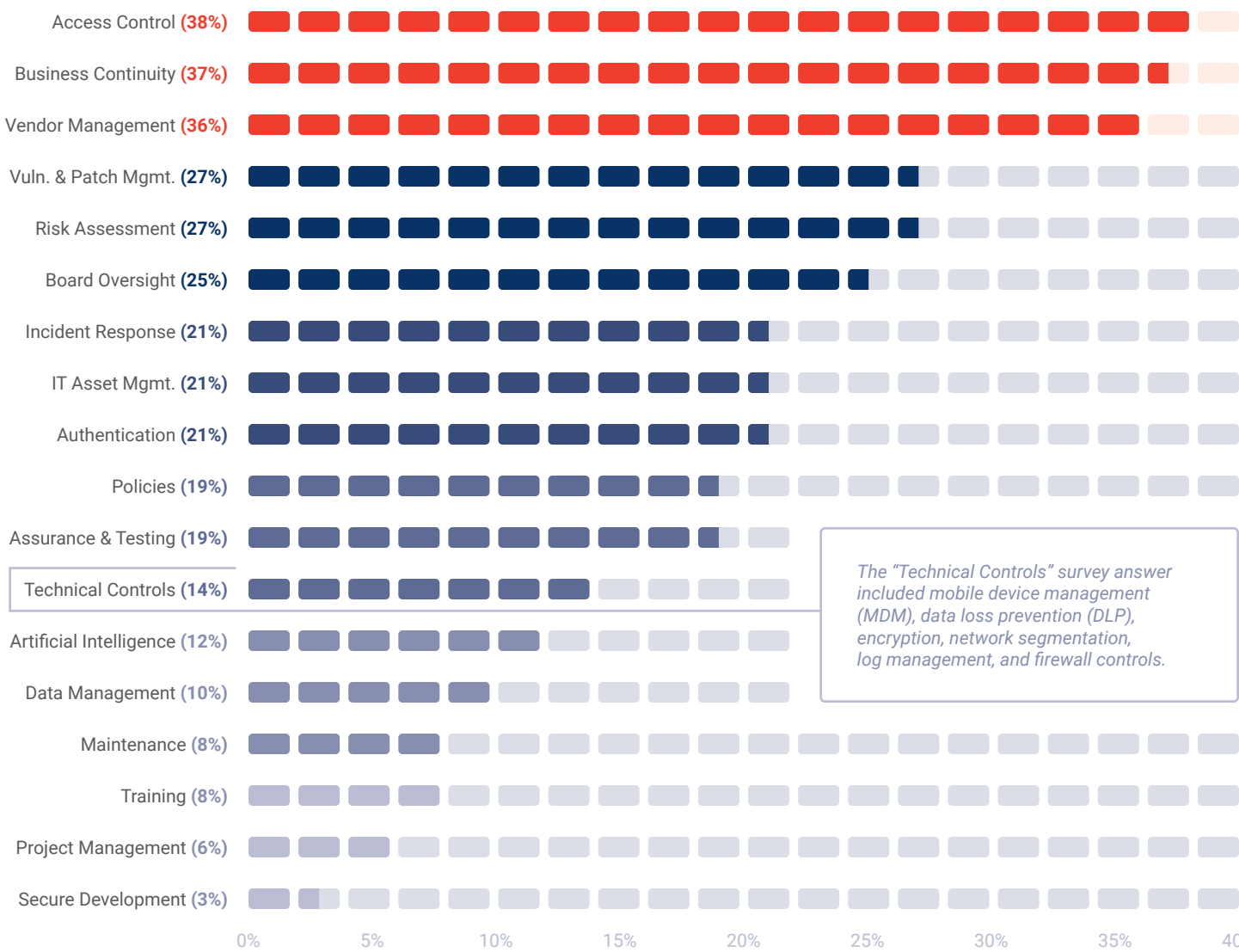
Examination priorities provide insight into the areas regulators are emphasizing during IT and cybersecurity reviews. To better understand current examination trends, we looked at what areas received the greatest focus from examiners during recent supervision activity.

Observation

Examination focus was distributed across several key risk areas.

When asked to identify up to five areas of focus during a recent examination, respondents most often selected access control (38%), business continuity (37%), and vendor management (36%). However, no single topic was identified by more than 38% of respondents, suggesting examiner attention remains distributed across a broad range of cybersecurity and compliance risks.

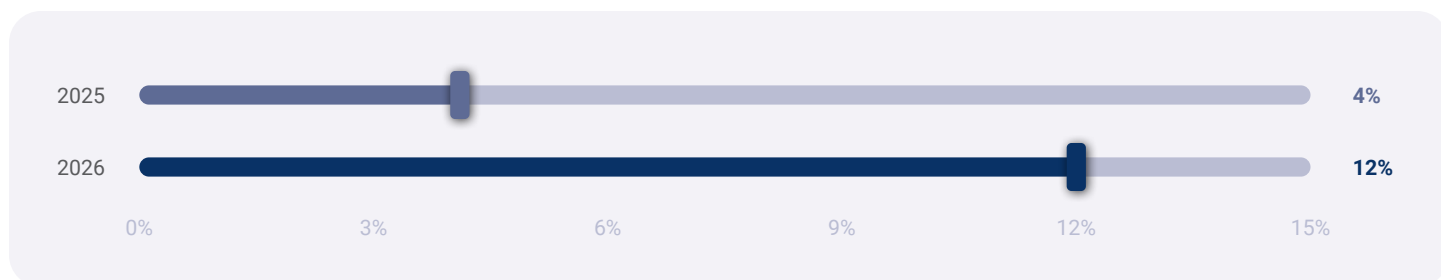
EXAMINATION PRIORITIES



Tuning In

Artificial intelligence was selected as a top examination priority by 12% of respondents, up from 4% in 2025. While AI remains a less common examination focus than other key areas, examiner attention to AI-related risks has increased significantly over the past year.

EXAMINATION FOCUS ON ARTIFICIAL INTELLIGENCE



Takeaway

No single topic appears to be driving examiner attention. Exam areas are spread across several areas of focus, suggesting regulators are taking a broad, risk-based approach rather than zeroing in on one issue.

What the data does tell us is that institutions preparing for their next exam should:

- **Focus on fundamentals.** Access control, business continuity, and vendor management topped the list of examination priorities, reinforcing the importance of maintaining strong foundational controls.
- **Keep documentation current.** Examiners continue to evaluate risk assessments, Board reporting, policies, and other governance activities. Well-maintained documentation helps demonstrate that cybersecurity risks are being actively managed.
- **Be prepared to discuss emerging risks.** While AI ranked lower overall, it was one of the fastest-growing examination topics. Be ready to explain how your institution evaluates and manages new technologies and emerging threats.

Examination priorities will continue to evolve. Institutions that focus on building a strong cybersecurity program rather than preparing for a specific examination topic will be better positioned to meet both cybersecurity and compliance expectations over time.

Compliance Monitoring

As the cybersecurity world changes, institutions must stay informed about how these changes may affect their compliance programs. To better understand how organizations monitor these developments, we looked at how respondents receive updates on compliance topics.

Observation

Institutions use multiple channels to stay current.

Compliance monitoring is supported by a mix of regulator-driven and industry-driven sources. Regulatory alerts (87%), information-sharing organizations (81%), and industry events (78%) were the most frequently cited resources, while 74% also subscribe to updates from vendors, service providers, or other third parties.

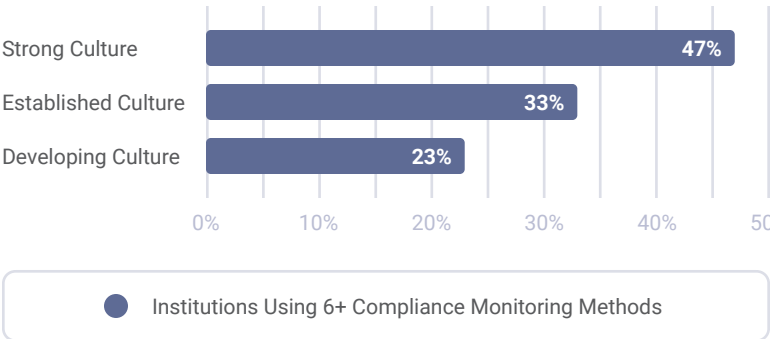
COMPLIANCE MONITORING CHANNELS



Tuning In

While developing cybersecurity programs are often driven by compliance requirements, institutions with stronger cybersecurity cultures reported the broadest use of compliance monitoring methods. Nearly half (47%) of respondents with a strong cybersecurity culture reported using six or more monitoring methods, compared to 33% of institutions with established cultures and 23% of those with developing cultures.

MONITORING METHODS BY CULTURE



Takeaway

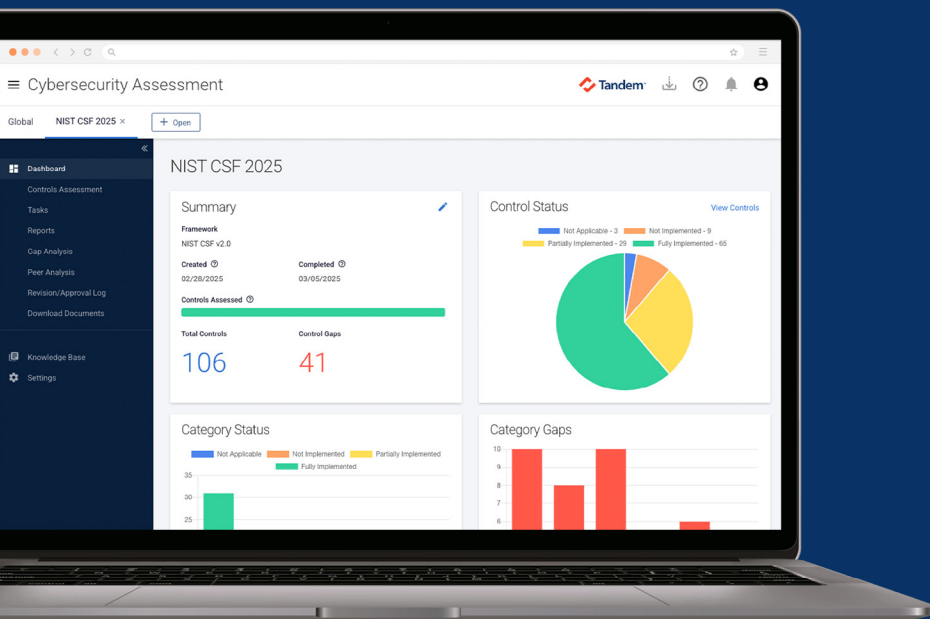
Most institutions are not relying on a single source to stay current with compliance changes. Instead, respondents reported using a variety of channels. While multiple sources can paint a more complete picture, they can also increase the amount of information institutions must review and process.

- **If your compliance monitoring program is mature**, periodically reassess the sources you monitor and focus on turning compliance updates into action.
- **If your compliance monitoring program is still developing**, identify a trusted set of sources, establish a consistent review process, and assign clear ownership for monitoring and communicating changes.

Compliance is one part of a larger cybersecurity picture. The real value comes not only from collecting the information, but from using it to make better decisions and strengthen your cybersecurity program.

TANDEM CYBERSECURITY ASSESSMENT

Perform self-assessments with ease.



Assess controls against 40+ frameworks

Perform gap and peer analysis

Create custom reports for stakeholders

Tandem.App/CA >

Simplify compliance with Tandem Cybersecurity Assessment.



Conclusion

At the beginning of this report, we asked the question: *“Are we the only ones trying to make sense of all this?”* Based on the data, the answer is clearly no, but the data points to something more specific than shared struggle.

What the Data Shows

Institutions know their strengths and weaknesses.

Maturity ratings were strong, but they weren't flat. Respondents rated security training and policies highest, with incident response and vendor management among the lowest. Those lower-rated areas share something in common: they are difficult to validate. An incident response plan cannot be proven until it is needed, and third-party risk depends (at least in part) on factors outside the institution's control.

Culture and engagement have outsized influence.

Whether the topic was Board oversight, program maturity, incident detection confidence, or compliance monitoring, institutions describing a strong cybersecurity culture and engaged leadership reported stronger programs across nearly every measure, regardless of team size or asset size.

Small teams are carrying a lot of weight.

Over a third of institutions have only one or two full-time IT and cybersecurity staff, and 78% of respondents wear two or more hats. Those same teams manage large vendor populations, multiple frameworks, and a growing list of AI considerations. It's a picture of resourcefulness under real resource constraints, and a reminder that strategic prioritization matters more than ever.

Third parties are extending the risk perimeter.

More than a third of institutions (35%) reported a significant impact from a third-party incident. Vendor management drew among the lowest maturity ratings in the survey and ranked among the top examination priorities. As institutions rely more on outside vendors (and those vendors rely more on AI), a growing share of risk sits outside the institution.

Artificial intelligence became operational.

Approved AI use climbed from 27% to 50% in a year while prohibition fell from 32% to 9%, and 90% now have an AI policy. However, 95% still cite cybersecurity, data exposure, and privacy as a concern, and 57% still acknowledge concern about weak AI governance, suggesting that policy has moved faster than practice.

Cutting Through the Noise

With so many priorities competing for limited resources, a few places stand out as good starting points:

- **A little evidence goes a long way.** If certain areas seem difficult to assess, you're not alone. Create opportunities to test your assumptions. Run a tabletop exercise. Review a critical vendor's controls. Pilot an AI use case and evaluate the results. When a program feels theoretical, look for ways to make it measurable.
- **Invest in culture.** A strong cybersecurity culture doesn't necessarily require a bigger budget or a bigger team; it requires consistent attention from leadership. Keep the Board engaged with regular reporting, and make cybersecurity part of everyday conversations, not just annual reviews.
- **Prioritize if your team is small.** No team can do everything perfectly, and lean teams have the least room to experiment. Focus first on the areas with the greatest potential impact rather than spreading limited time evenly across every responsibility.
- **Treat vendor oversight as risk management, not a compliance checkbox.** As more risk lives outside your institution, your vendor management program needs to keep pace. Make sure critical vendors receive real supervision, and start asking vendors directly how they're using AI.
- **Get ahead of AI governance while it's still manageable.** Employees are already using AI tools, approved or not. Institutions that build visibility into both approved and unapproved use will be better positioned than those waiting for policy to catch up with reality.

Taken together, these findings point to a single conclusion. The institutions navigating 2026 most effectively aren't the ones with the biggest budgets or the largest teams. They're the ones focusing on the right things and doing them to the best of their ability.

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.



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.



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. Savannah currently works as a GRC Content Analyst, where she helps create and maintain cybersecurity and compliance content for Tandem. Her enthusiasm for learning shows with interest in topics such as GRC, risk management, and personal financial planning.



MORGAN MARET, ITRF
Software Specialist

Morgan is passionate about learning and helping others navigate complex challenges. She is a Software Specialist at Tandem with a B.A. in Psychology and has earned the IT Risk Fundamentals ISACA Certificate. With a natural curiosity and analytical mindset, Morgan enjoys investigating issues, identifying root causes, and developing practical solutions to difficult problems. Outside of work, find her hiking or following advancements in space exploration.



JACOB JONES
Developer

Jacob has spent the past eight years as a developer at Tandem, building solutions that help financial institutions navigate governance, risk, and compliance. He holds a B.S. in Computer Science, which grounds his approach to solving technical challenges for Tandem's clients. Outside of work, Jacob is a husband, girl dad, and enjoys family time, sports, and dabbling in all kinds of art.

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.



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 assessments. 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

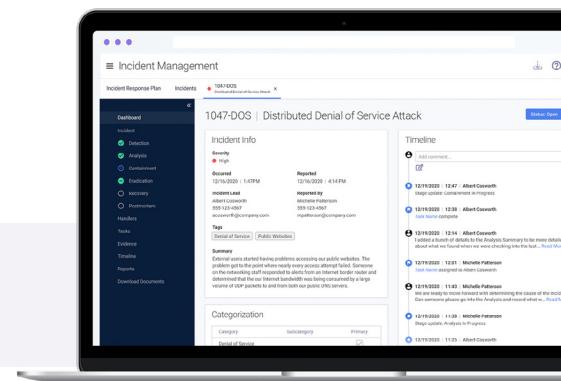
Perform information security and asset-based risk assessments with our easy-to-follow format and available templates.



VENDOR MANAGEMENT

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

Ready to see how Tandem can help? Schedule a demo at Tandem.App/Demo.





Copyright © Tandem, LLC. 2026.09.v1
info@tandem.app
844-698-9800