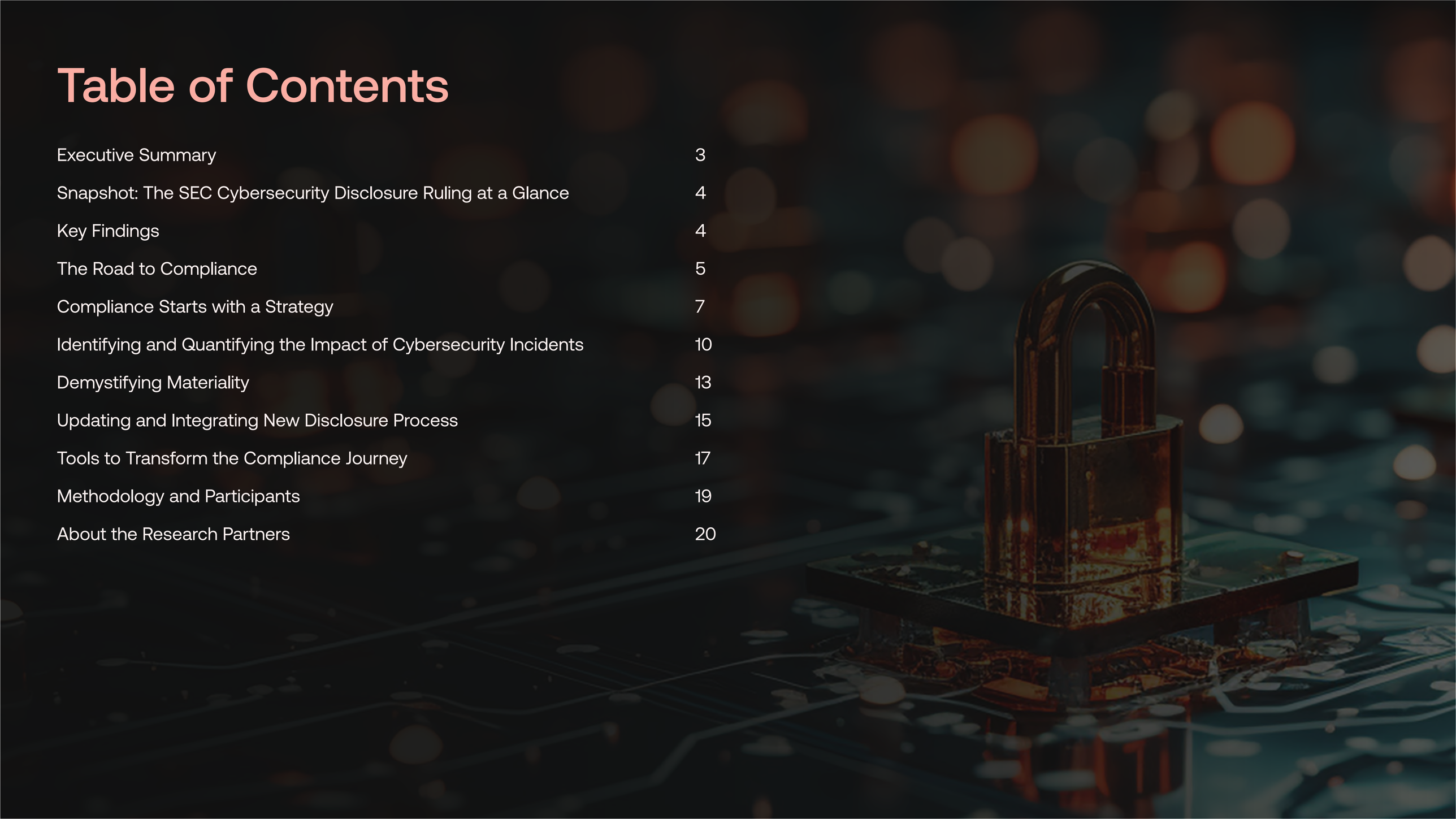
Decode the New SEC Cybersecurity Disclosure Ruling

AUDITBOARD | Ascend2 RESEARCH-BASED MARKETING

Table of Contents



Executive Summary

AuditBoard's new report in collaboration with Ascend2, *Decode the New SEC Cybersecurity Disclosure Ruling*, reveals that 68% of survey respondents are overwhelmed by the new U.S. Securities and Exchange Commission (SEC) cybersecurity disclosure ruling established in October 2023.

In January 2024, AuditBoard surveyed over 300 security professionals who are closest to the efforts their organizations are implementing to comply with this new ruling. These professionals largely represented enterprise companies in the U.S. with over $100M in annual revenue, spanning several industries, roles - including senior leadership and executives, and departments.

Many executives are still in the initial stages of conducting gap assessments, assigning responsibility for remediation, establishing standards for determining materiality, creating new disclosure processes, and implementing technology.

According to the data, IT risk and compliance leaders:

- **Anticipate significant impact on their business** as a result of the new SEC cybersecurity disclosure ruling and resulting process changes.
- **Emphasize the importance of an underlying strategic approach** built on a foundation of tools to help standardize and capture processes across teams.
- **Prioritize the right technology** to increase confidence in their ability to comply with the new ruling.

Decode the New Cybersecurity Disclosure Ruling assesses progress made by companies working to comply, the challenges they face, and provides recommendations for actionable steps toward implementation. AuditBoard provides all the steps to empower your organization to conduct gap assessments, create a compliance strategy, identify the impact of cybersecurity incidents, demystify and define materiality, integrate disclosure processes, and transform your technology with the right tools.

Snapshot: The SEC Cybersecurity Disclosure Ruling at a Glance

The SEC cybersecurity ruling mandates that publicly traded companies disclose significant cybersecurity incidents in a timely manner, along with the measures taken to address these threats. This ruling underscores the importance of cybersecurity as a critical aspect of corporate governance and investor protection. It aims to enhance transparency and accountability in cybersecurity practices among publicly traded companies, ultimately safeguarding investors' interests and promoting market integrity.

Publicly traded companies are not the only ones being impacted. The new ruling also includes high-level disclosures involving third-party vendors of these organizations. Needless to say, the requirements to comply with the new SEC cybersecurity disclosure ruling have created a ripple effect that reaches deep within these organizations and outside of them to the companies that support them.

Key Findings

- **If you haven't already, the time is now to implement compliance efforts.**
  While 98% of security professionals and executives surveyed have started working to comply with the new SEC cybersecurity disclosure ruling, over one-third are still in the early phases of their efforts.
- **Performing gap assessments sets you on the right track.**
  Less than half (48%) of organizations have performed a gap assessment to determine what needs remediation to comply. Those who have, however, are significantly more confident in their ability to comply with the new ruling in 2024 than those who have not.
- **Materiality may be vague, but using a framework can help provide context.**
  49% of organizations have already established processes and methodologies to determine materiality, and 98% of those using a materiality framework report a moderate to high understanding of that framework and their ability to provide the right inputs.
- **Potential roadblock: Departmental alignment to update the disclosure process.**
  Updating or integrating the disclosure process is a top challenge, and only 39% of organizations have cross-functional/departmental alignment on processes and steps.
- **Using the right technology matters.**
  An integrated view of risk management significantly increases confidence in complying with the new SEC cybersecurity ruling in 2024. Further, those using technology to facilitate the disclosure process feel less challenged by stakeholder adoption of these new workflows.

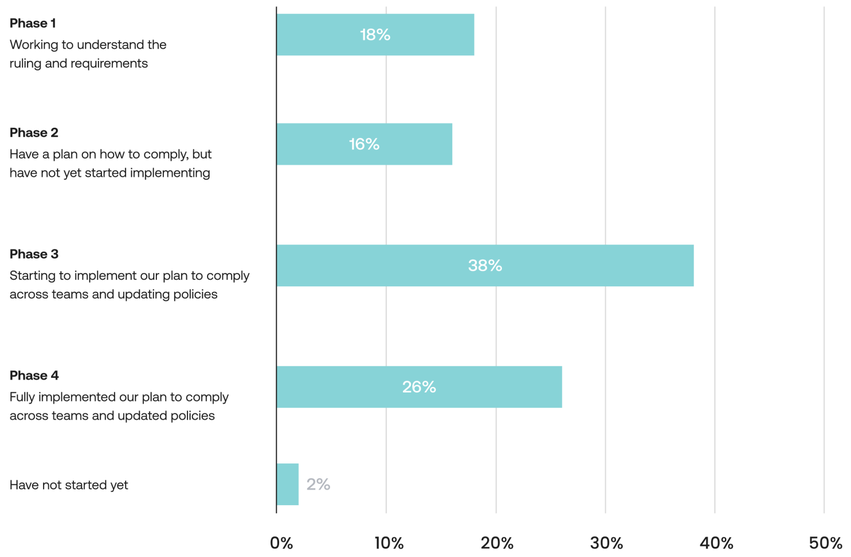
The Road to Compliance

Where are companies on their compliance journey?

Nearly all organizations surveyed have embarked on their journey to compliance with the new SEC cybersecurity disclosure ruling. However, one-third (34%) are still in the early stages of their efforts, with 18% of those surveyed still working to understand the ruling and requirements and another 16% saying they have a plan to comply but have not yet started implementing.

The rest have started implementing their plan to comply (38%) or are currently operating with a fully implemented compliance plan (26%).

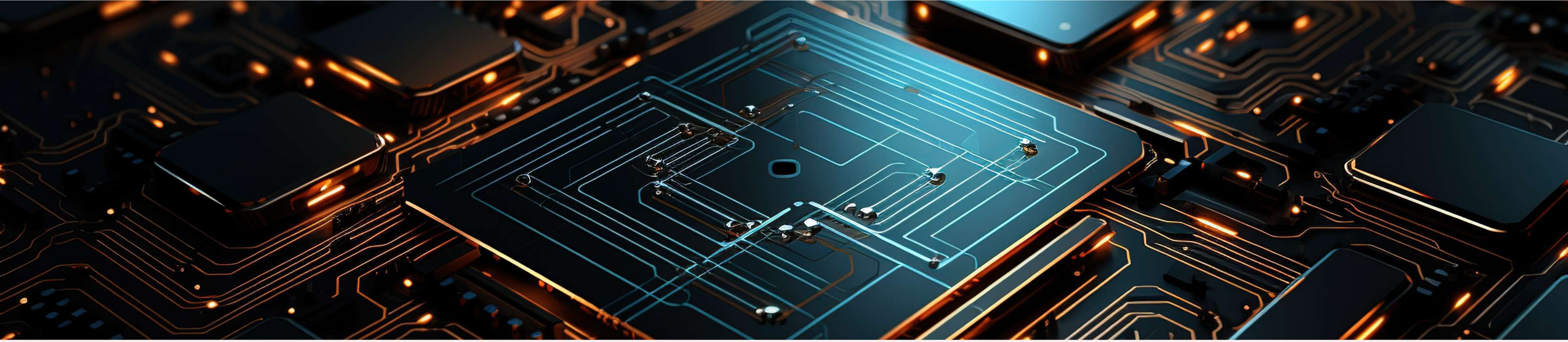
Figure 1. *Which phase best describes where your organization is in the process to comply with the SEC cybersecurity disclosure ruling?*



Implementing compliance efforts takes time.
Overall, 60% of security professionals and executives had been working on efforts to comply with the new SEC cybersecurity disclosure ruling for over 6 months. However, 82% of those who have fully implemented plans and policies across teams (Phase 4) have been working on this for over 6 months, with 50% reporting that this work has been ongoing for over a year.

Figure 2. *How long have you been working on efforts to comply with the SEC cybersecurity disclosure ruling? (Segmented by maturity phase)*

	PHASE 1	PHASE 2	PHASE 3	PHASE 4
Less than 3 months	28%	14%	6%	2%
3 - 6 months	26%	34%	34%	15%
6 - 12 months	18%	40%	46%	32%
Longer than 12 months	26%	12%	14%	50%



Maturity Snapshot

- **Public companies** are more advanced in their compliance journey than private companies. 73% of public companies have at least started implementing their plan to comply (44% have started and 29% have fully implemented plans and policies) vs. just 59% of private companies (34% have started and 25% have fully implemented plans and policies).

- **Compliance maturity also varies by industry.** The most advanced industry is **finance and insurance**, with 73% of finance and insurance professionals reporting that they have either started to implement or have a fully implemented plan to comply. The least mature is the **technology** industry, with only 52% of technology professionals reporting having started or fully implemented a plan to comply.

- **Smaller companies** (those with under 1000 employees or with less than $500M in revenue) are more likely to report being in the early stages of their compliance journey than those with larger revenues and higher employee counts.

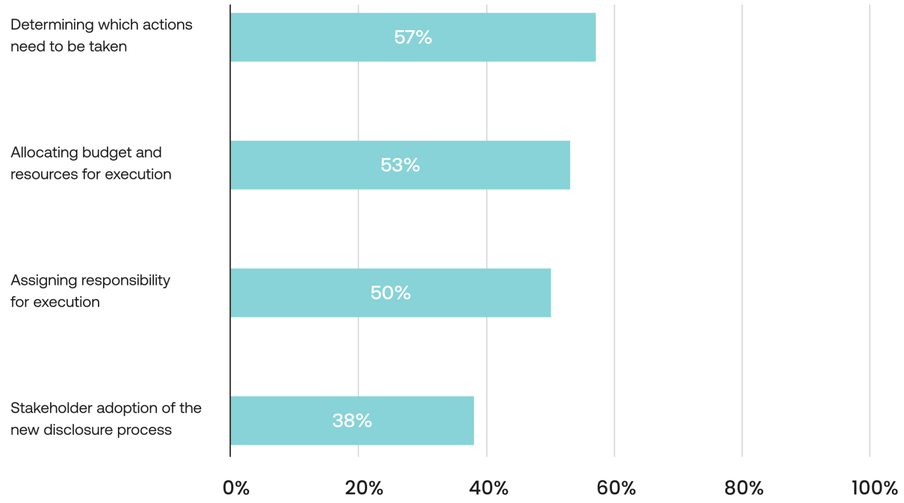
Compliance Starts with a Strategy

Regardless of where a company is on its road to compliance, the importance of starting this journey with a strategy to execute these initiatives cannot be understated.

Establishing what needs to happen and when is a critical first step and will be a demanding task for security professionals and executives in the coming year. In fact, over half (57%) of those surveyed report that determining which actions must be taken will be a top challenge as they work to comply with the new SEC cybersecurity ruling in 2024.

Allocating the budget and resources required for executing new processes and assigning responsibility for actions are also recognized as top compliance challenges for the coming year. Fortunately, with the right tools and well-developed infrastructure, new compliance processes can be streamlined, and reporting resources can be augmented to help alleviate these barriers to success.

Figure 3. *Which of the following do you expect to be a challenge as you work to comply with the SEC cybersecurity ruling in 2024?*



Developing a strategy to take action

1. Conduct gap assessments of current workflows and processes to determine your ability to report on cybersecurity and risk and to disclose any cybersecurity events within the time allotted by the SEC. Identify what needs to be updated or implemented to comply.
2. Define your organization's method for determining materiality. Assign responsibility and how long their process should take, using frameworks to provide context.
3. Determine what the disclosure process should look like. Who will draft, review, approve, and publish the final disclosure? How long do they have to execute?
4. Connect the dots to create a streamlined workflow across all teams involved. There should be procedures and timelines for the execution and hand-off from one stage to the next, from your cybersecurity teams that detect incidents to the teams that determine whether those incidents are material to the teams involved in the disclosure process.
5. Test your processes. Simulate an incident and run it through your new workflow to ensure there are no bottlenecks or gaps and that the disclosure can happen within the timeframe allotted by the SEC.
6. Refine, optimize, repeat.

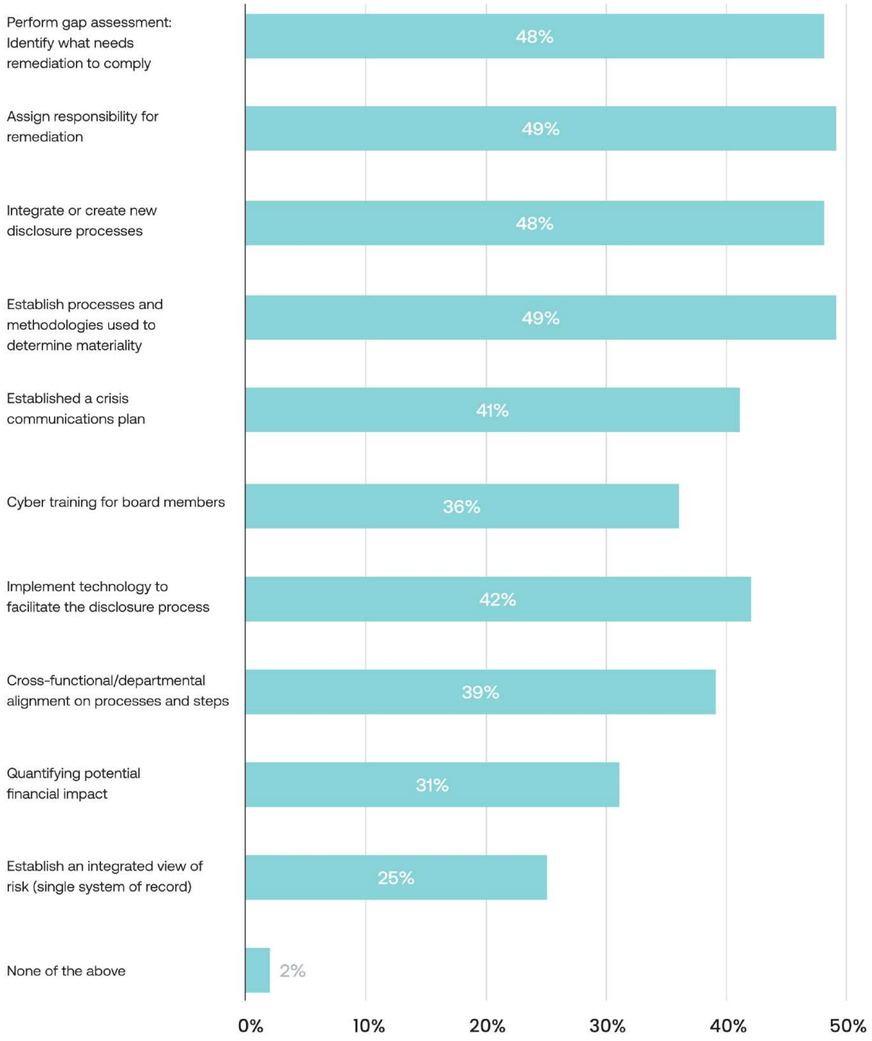
Gap assessment and assigning responsibility for remediation.

A critical early-stage action that companies should be taking to help determine and prioritize compliance initiatives is performing a gap assessment. These assessments can be used to form the foundation of a compliance strategy. However, only about half (48%) of those surveyed have performed a gap assessment to determine what needs remediation to comply with the SEC's new ruling. Another 49% say they have taken the next step and assigned responsibility for remediation. Over half of those who have not taken these actions plan to do so in the first half of 2024.

Actions around determining materiality, updating disclosure processes, and using technology to facilitate the disclosure process have also occurred for about half of those surveyed.

Performing gap assessments increases confidence in your organization's ability to comply. Security professionals and executives who report having performed a gap assessment are significantly more likely to be highly confident in their company's ability to comply with the new SEC cybersecurity disclosure ruling than those who have not performed a gap assessment (61% vs 48%).

Figure 4. *What actions has your organization taken to address the SEC cybersecurity disclosure ruling?*



Evolving compliance maturity.

As companies progress through compliance efforts, moving from the early phases of pre-implementation and planning into the execution phases, we see significant increases in actions taken. Notably, companies in more mature stages of compliance seem to have focused heavily on **establishing processes used to determine materiality** and **integrating or creating new disclosure processes**. These two critical elements of compliance with the new SEC cybersecurity disclosure ruling are key differentiators between companies in the planning stage and those who have started implementing.

Companies in the later execution phases are also over 3x more likely than those in earlier phases to have established an integrated view of risk and nearly 2x more likely to have cross-functional and departmental alignment on processes and steps that need to be taken to comply.

Figure 5. *What actions has your organization taken to address the SEC cybersecurity disclosure ruling? (Segmented by maturity phase)*

	PHASE 1 & 2	PHASE 3 & 4
Perform gap assessment: Identify what needs remediation to comply	44%	51%
Assign responsibility for remediation	47%	52%
Integrate or create new disclosure processes	39%	54%
Establish processes and methodologies used to determine materiality	38%	56%
Established a crisis communications plan	32%	46%
Cyber training for board members	29%	41%
Implement technology to facilitate the disclosure process	30%	49%
Cross-functional/departmental alignment on processes and steps	25%	47%
Quantifying potential financial impact	27%	32%
Establish an integrated view of risk (single system of record)	10%	33%

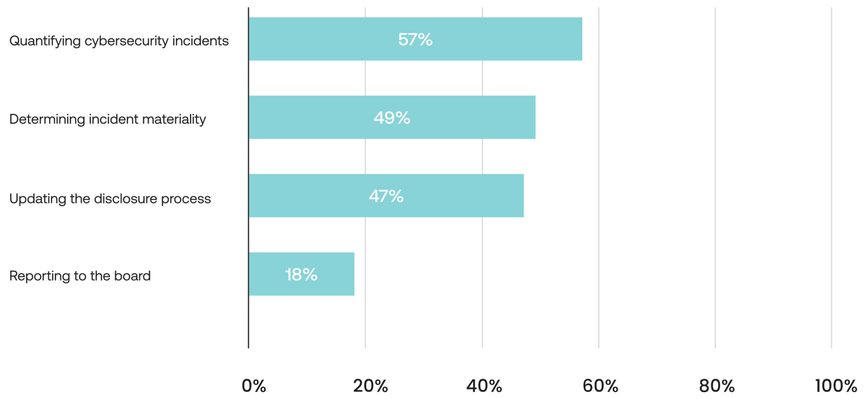
Identifying and Quantifying the Impact of Cybersecurity Incidents

Gauging the impact of cybersecurity incidents.

The new SEC cybersecurity disclosure ruling requires companies to identify and disclose material cybersecurity incidents. This means organizations need to rethink how they determine the size of the impact of each incident, which could have quantitative factors, for example, the impact on stock price. As a result, risk quantification is top of mind for companies as they think through the new regulations.

Quantifying the impact of cybersecurity incidents is the most commonly reported challenge of complying with the SEC cybersecurity disclosure ruling, as reported by 57% of those surveyed. Gaining a clear understanding of the impact of cybersecurity incidents on the business is critical to the disclosure process.

Figure 6. *What are your biggest challenges in complying with the SEC cybersecurity disclosure ruling?*



CLARIFYING MATERIALITY.

Organizations need to determine what materiality looks like in the context of their business and industry, and every determination will look different. Still, creating clear definitions and guidelines is essential to effectively quantifying the impact of cybersecurity incidents. Ask questions such as:

- Would this incident impact stock price if stakeholders knew about it?
- Does this incident damage our reputation?
- Does this incident expose customer data?

Organizations should ensure that answering these types of questions relevant to their specific business and industry can determine whether an incident meets their materiality thresholds.

Perceived top challenges vary by job level. Executives are significantly more burdened than other cohorts by reporting to the board (25% of executives report this as a top challenge vs 17% of senior leadership and 13% of management). Updating the disclosure process is senior leadership's top challenge, with 61% listing it as such (compared to just 38% of executives and 45% of management).

Less than one-third (31%) of security professionals and executives say they have the ability to quantify the potential financial impact of cyber risks.

Quantifying the impact of cybersecurity incidents requires a comprehensive and integrated view of cybersecurity risk across the entire organization. Integrated Risk Management (IRM) provides this view, allowing companies to identify cybersecurity incidents and risks, gauge potential impact, and manage material risks. Implementing an IRM approach enables teams to share data in a single system of record, greatly improving data integrity and efficiency of disclosures.

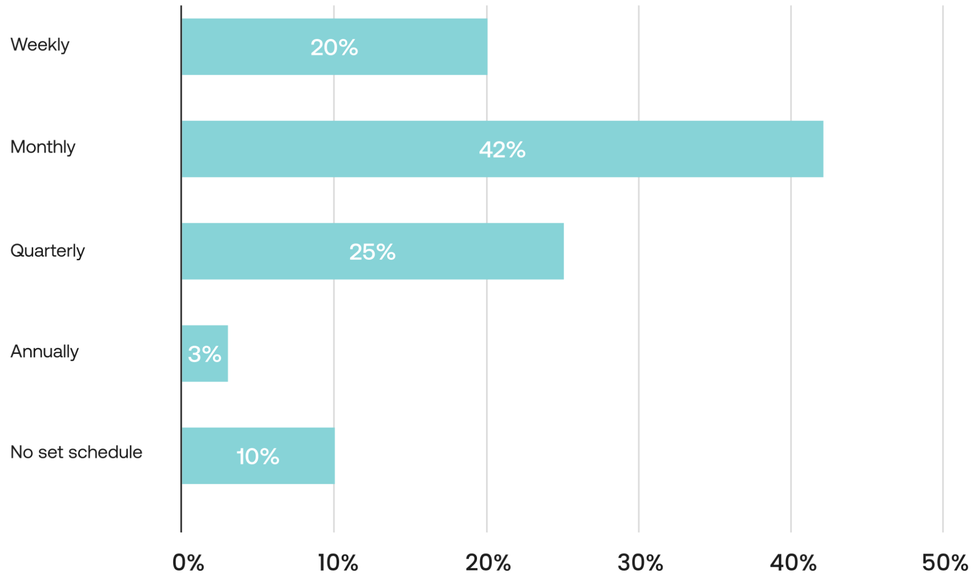
Incident response and crisis management.

93% of security professionals and executives surveyed agree that training and testing incident response is critical to an effective cybersecurity framework. Incident simulations help teams understand guidance on confirming materiality with realistic scenarios and help cross-functional teams understand their roles in supporting the publishing of a disclosure.

> More testing means more confidence. The more often an organization tests its new incident response plan, the more confident those surveyed are in its ability to comply with the new SEC cybersecurity disclosure ruling. 75% of those who test their plan weekly are highly confident vs just 49% of those testing less frequently.

The most common schedule for testing incident response plans is monthly, according to those surveyed (42%). Another one-quarter are testing quarterly. One in ten companies report having no set schedule.

Figure 7. *How often are you testing your new incident response plan?*



RUNNING AN INCIDENT SIMULATION.

Now that you have defined your roles and processes, it is time to test your procedures and workflows. Doing so provides valuable insight into areas that need improvement and establishes a clear understanding of what is required of everyone involved. Here are some tips to make incident testing more effective:

- Define roles and expectations and involve every individual the process touches in your simulation. This ensures that everyone understands what their roles and responsibilities are.
- Give responsible parties the space to understand what to expect. Running your simulation in a low-stress environment (rather than waiting to see what happens during an actual incident) provides clarity of mind and allows all involved to understand what to expect and what is expected of them.
- Pressure test the guidance in your plan. Are expectations consistent across workflows? Or are different teams arriving at different conclusions? If the latter is the case, it may be a sign that your guidance is not specific enough.
- Test for timing. Determine whether you can meet the tight timelines allotted by the SEC. If you are continuously lagging in this area, consider increasing the sense of urgency you impart to those involved. Other important considerations include evaluating whether you have the right people and technology to facilitate these processes effectively. Additional people, processes, or technology investments may be necessary to close the gap.

81% of those surveyed feel that the SEC cybersecurity disclosure ruling has a moderate or significant impact on existing crisis management or business continuity processes.

59% of those surveyed have not yet established a crisis communications plan, but of this group, 56% plan to do so in the first half of 2024.

Demystifying Materiality

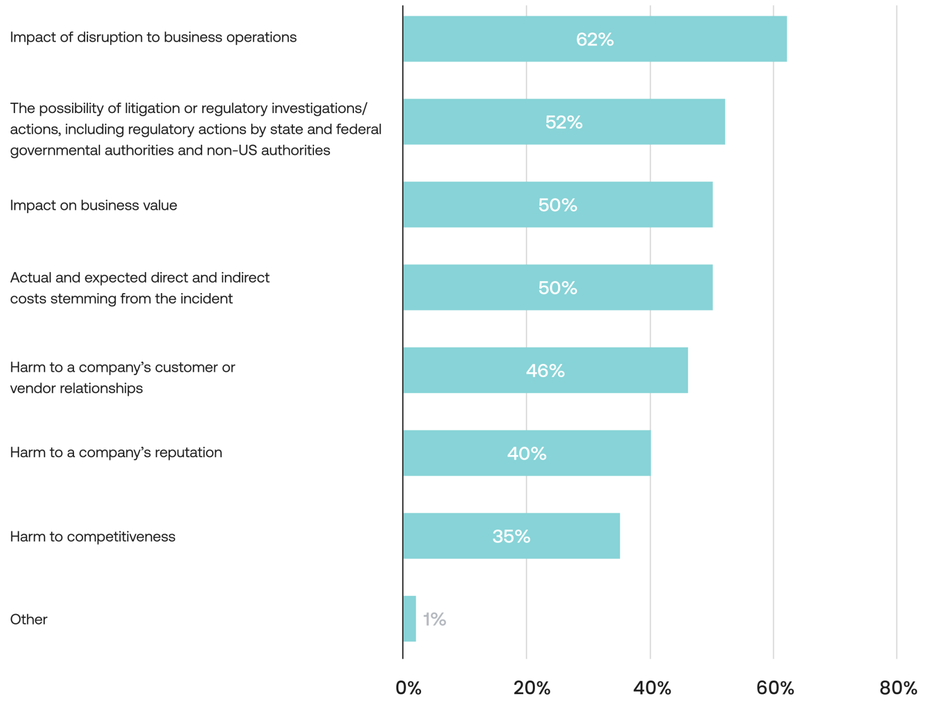
Identifying material cybersecurity incidents.

The new SEC cybersecurity disclosure ruling requires the disclosure of material cybersecurity incidents but includes no set definition of what qualifies an incident as “material” outside of it impacting shareholders. This is largely left up to individual organizations and ranks among the most significant challenges associated with compliance efforts.

Nearly half (49%) of companies surveyed have already established processes and methodologies to determine materiality, and 54% of those that haven’t plan to do so in the first half of 2024.

When determining materiality, which attributes are being considered by most organizations? The impact of the incident’s disruption on business operations, the possibility of litigation or regulatory investigations/actions, the impact on business value, and actual and expected costs associated with the incident are all top considerations when evaluating materiality, according to security professionals and executives surveyed.

Figure 8. *What are you considering when evaluating materiality?*



Those in the most mature stage of their process to comply with the SEC disclosure ruling (Phase 4) are more likely than others to consider all of the above attributes when evaluating materiality. However, this group places significantly more weight on harm to a company’s customer or vendor relationships than those in earlier stages.

Figure 9. *What are you considering when evaluating materiality? (Segmented by maturity phase)*

	PHASE 1	PHASE 2	PHASE 3	PHASE 4
Impact of disruption to business operations	53%	56%	63%	68%
The possibility of litigation or regulatory investigations/actions, including regulatory actions by state and federal governmental authorities and non-US authorities	42%	38%	55%	62%
Actual and expected direct and indirect costs stemming from the incident	42%	42%	52%	60%
Harm to a company's customer or vendor relationships	40%	36%	46%	59%
Impact on business value	44%	44%	55%	55%
Harm to a company's reputation	39%	36%	40%	46%
Harm to competitiveness	30%	34%	33%	41%

The benefits of using a materiality framework.

Materiality frameworks can be a helpful system to provide context for determining which incidents are indeed material. In fact, 58% of security professionals and executives surveyed are using a materiality framework… and those who are, have significantly more confidence in their company's ability to comply with the new SEC cybersecurity disclosure ruling in 2024. Nearly two-thirds (63%) of those with a materiality framework have high confidence in their ability to comply with the new ruling vs 41% of those working without a framework.

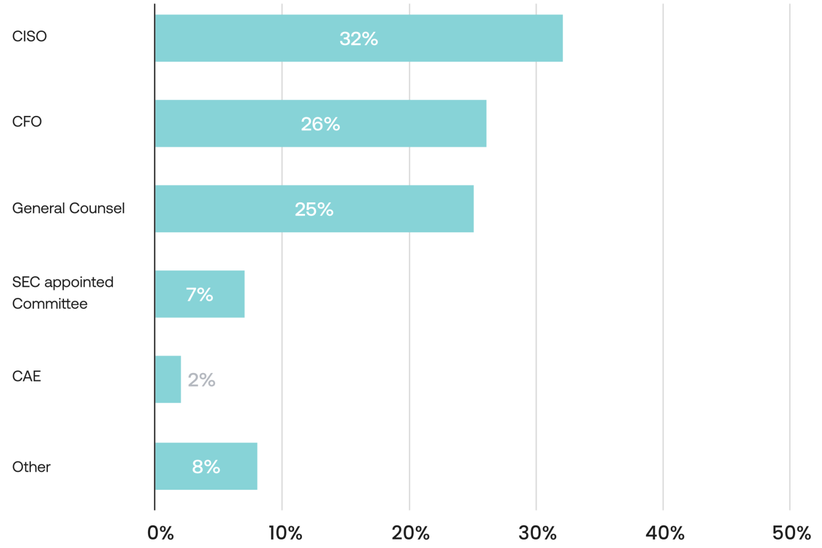
Those with a materiality framework have a good understanding of what it consists of and what they need to use it effectively. 98% of those using a materiality framework report a moderate to high understanding of their company's materiality framework and ability to provide the right inputs.

CISOS MAY BE UNDER THE MOST PRESSURE.

The CISO is the most commonly reported position responsible for determining materiality (32%). CISOs have a personal liability risk if they get this determination wrong or do not have enough influence to trigger a disclosure when necessary. With these decisions under the scrutiny of the SEC, and CISOs being held liable for anything deemed a failure, tensions have developed between CISOs and their organizations.

The even distribution of primary responsibility between CISO, CFO, and General Counsel reveals that various corporate structures can be used to manage the process of determining materiality. Regardless of where the responsibility lies, this liability risk will undoubtedly be a continuing conversation in the coming months as organizations work through compliance efforts and refinement.

Figure 10. *Who is primarily responsible for determining materiality?*



Updating and Integrating New Disclosure Processes

Updating the disclosure process.

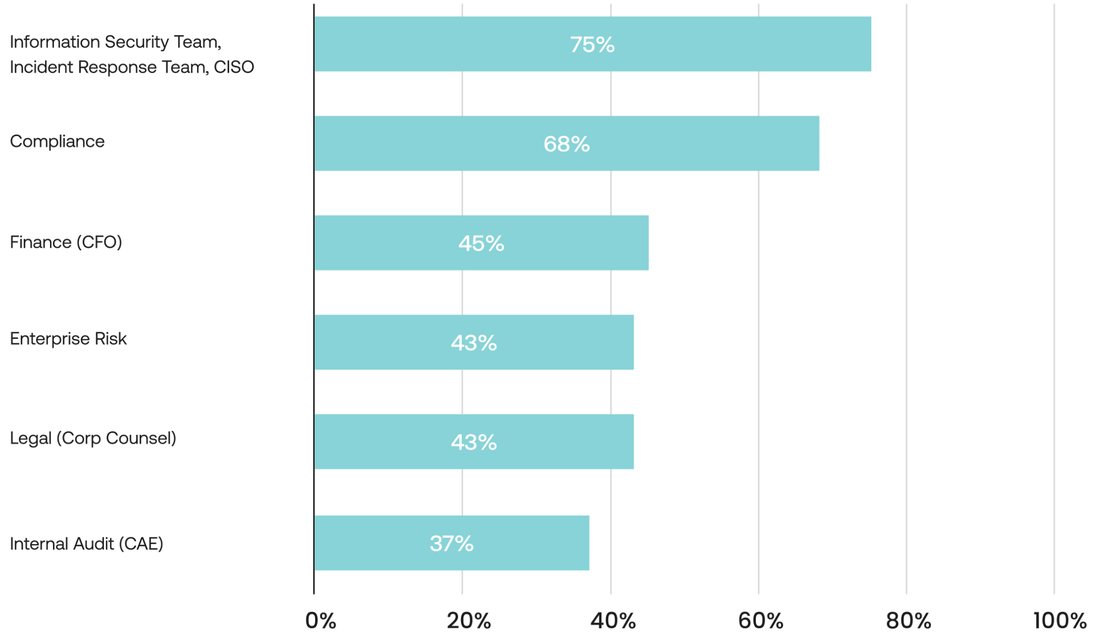
Organizations will need to identify how a new cybersecurity disclosure process will integrate or align with existing disclosure processes, which is proving to be a top challenge, according to those surveyed. Less than half (48%) of security professionals and executives surveyed report having already integrated or created new disclosure processes as a part of their journey to compliance. However, 48% of those who have not done so plan to do so in the first half of 2024.

Stakeholder adoption of new disclosure processes is expected to be a top issue moving forward, according to 38% of those surveyed.

WHO IS INVOLVED IN THE DISCLOSURE PROCESS?

According to security professionals and executives surveyed, the Information Security Team/Incident Response Team/CISO is the most heavily involved in the SEC cybersecurity disclosure process. Compliance is also involved for over two-thirds of organizations. Less than half (45%) of companies involve finance teams, and only 37% report involving internal audit.

Figure 11. *Who is involved in the SEC cybersecurity disclosure process?*



Teams involved in the disclosure process vary based on stage of maturity in the process to comply with the SEC ruling. Interestingly, we see a drop-off in those who involve their legal, internal audit, and finance teams from Phase 3 to Phase 4.

Figure 12	PHASE 1	PHASE 2	PHASE 3	PHASE 4
Information Security Team, Incident Response Team, CISO	60%	70%	82%	80%
Compliance	63%	56%	71%	77%
Enterprise Risk	37%	34%	45%	51%
Legal (Corp Counsel)	28%	40%	50%	46%
Internal Audit (CAE)	19%	34%	44%	41%
Finance (CFO)	37%	60%	48%	35%

50% of organizations extend their cyber policies, procedures, and practices to all third-party vendors. Another 40% are currently extending their practices to some third-party vendors.

Involving the board.

Over half (53%) of security professionals and executives report having someone with cybersecurity expertise on their board of directors. However, just 36% of those surveyed say that their organization provides cyber training to board members to educate them on cybersecurity practices, risks, and procedures.

Those educating their board, however, are more confident in their organization's ability to comply with the SEC ruling in the coming year. 61% of those providing cyber training to board members are highly confident in their company's ability to comply with the new SEC cybersecurity ruling in 2024 compared to 51% of those not providing training.

Tools to Support the Compliance Journey

Organizational alignment is critical to understanding and reporting risk.

Data integration and alignment across teams are not only essential in mapping out the processes involved in the road to compliance, but they are also critical to creating a holistic view of risk posture. Still, only 39% of executives and security professionals surveyed report that their organization has cross-functional/departmental alignment on processes and steps.

Just 39% of organizations have cross-functional and departmental alignment on processes and steps.

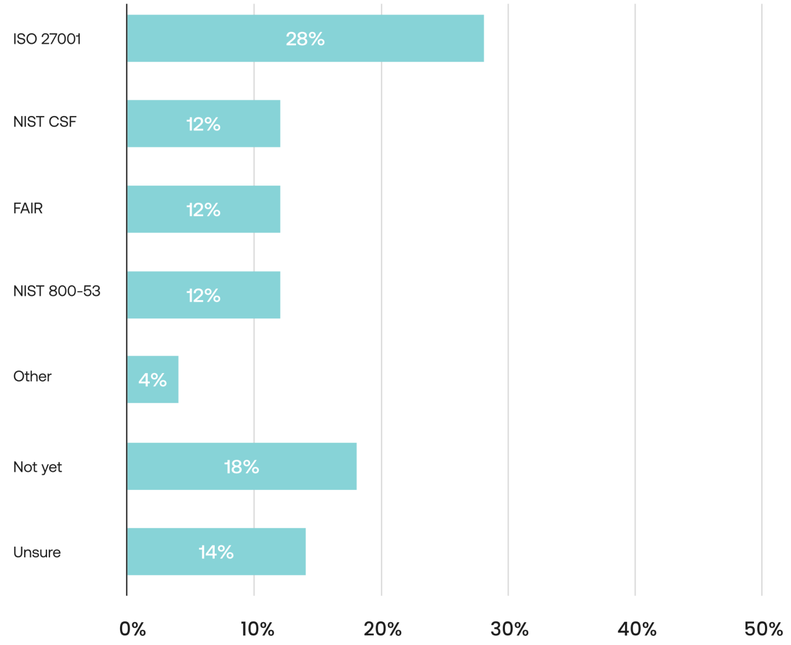
As companies move toward compliance readiness, the need to streamline incident data collection, gap analysis, and issue remediation becomes more apparent. Investing in tools that help standardize these processes can align efforts across teams to create efficiencies, encourage stakeholder adoption, and improve the ability to comply with the new SEC cybersecurity disclosure ruling. While the vast majority of those surveyed have some extent of understanding of their company's cyber risk posture and risk management program, only 54% report a high understanding.

Executive perspective

Executives understand their risk posture and management program most, with 71% reporting a high understanding. This is compared to 59% of senior leadership respondents and just 42% of management professionals. A cross-functional and cross-departmental understanding of an organization's risk management is important in effectively mitigating future risk.

How are companies evaluating risk posture? The most common risk model used to evaluate cyber risk posture is ISO 27001, used by 28% of those surveyed. Nearly one in five report that they do not yet use criteria to evaluate risk posture.

Figure 13. *Is there a criteria you evaluate your cyber risk posture against?*



Adopting the Right Technology to Align Compliance Efforts

Adopting technology is essential for aligning compliance efforts with the SEC Cybersecurity ruling, as it enables organizations to automate data collection, analysis, and reporting processes, ensuring timely and accurate disclosure of cybersecurity incidents. Meeting the SEC's requirements will involve adopting an integrated compliance management software to ensure that disclosure is accurate, complete, and transparent – and pulled together in a timely manner.

TECHNOLOGY TO SUPPORT THE DISCLOSURE PROCESS.

42% of security professionals and executives surveyed report that their organization has already implemented technology to facilitate the disclosure process, leaving 58% of organizations that have not. However, 44% of those who have not yet implemented this technology plan to do so in the first half of 2024.

Organizations must disclose material incidents promptly to comply with the new SEC cybersecurity disclosure ruling. Adopting technology to support this can greatly reduce the timing of the disclosure process by enabling standardization and streamlined reporting across teams. In fact, senior leadership and executives who report using technology to facilitate disclosure workflows feel less challenged (37%) by stakeholder adoption of the disclosure process than those who have not implemented this technology (43%).

TECHNOLOGY TO ENABLE AN INTEGRATED VIEW OF RISK.

Three-quarters (75%) of organizations do not yet have a single system of record for risk management. Obtaining this integrated view, whether through a single integrated solution or several solutions tied together, is becoming more of a priority.

Why an integrated view? Those with a single system of record for risk management have significantly more confidence in their company's ability to comply with the new SEC cybersecurity ruling in 2024 than those without. Two-thirds (65%) of security professionals and executives surveyed with an integrated view of risk report being highly confident in their company's ability to comply compared to just 50% of those without.

The right technology stack will play an integral role in complying with the SEC's new cybersecurity disclosure ruling and help organizations evolve with the landscape of cybersecurity regulations rather than try to catch up with it.

Methodology and Participants

Methodology

AuditBoard, in partnership with Ascend2 Research, developed a custom online questionnaire to survey 314 security professionals working for enterprise organizations with over $100M in revenue (96%) across varying industries in the United States. These individuals largely represented roles of manager and above (98%). All survey participants confirmed their knowledge of how their business is complying or planning to comply with the new SEC cybersecurity disclosure ruling. The survey was fielded in January 2024.

Participants

Industry

Industrial (e.g., manufacturing, utilities, mining/quarrying/oil and gas extraction, construction, transportation/warehousing, waste management/ remediation services)	26%
Technology (e.g., communications equipment, IT services, software, technology hardware)	26%
Finance and insurance (e.g., financial institutions, insurance, asset management, broker-dealers)	14%
Services (e.g., healthcare, retail trade, real estate, hospitality, wholesale trade, entertainment, information, professional, agriculture)	20%
Government and education (e.g., public administration, educational services)	9%
Other	5%

Annual Revenue

Less than $100M	4%
$100M - $499.99M	14%
$500M - $999.99M	29%
$1B - $2.499B	20%
$2.5B - $9.99B	16%
$10B or more	17%

Holding

Publicly traded for profit	40%
Privately held for profit	46%
Not-for-profit	6%
Public sector	8%

Primary area of focus

Sustainability	1%
Finance	19%
Legal	3%
IT	38%
InfoSec	2%
Compliance	17%
Risk Management	7%
Internal Audit	3%
Other	10%

Job Level

Executive	25%
Senior Leadership	30%
Management	43%
Individual Contributor	2%

Number of employees

1 - 99 employees	4%
100 - 999 employees	23%
1,000 - 9,999 employees	44%
10,000 or more employees	29%

About the Research Partners

AUDITBOARD

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.

Ascend2™
RESEARCH-BASED MARKETING

Companies partner with Ascend2 to create original research from survey conceptualization through report and content creation to media outreach. Ascend2 helps companies fuel marketing content, generate leads, and engage prospects to drive demand through the middle of the funnel. For more about Ascend, visit ascend2.com.