Gartner
Peer Community™

Cyber Risk Quantification: Adoption and Impacts

How are organizations employing cyber risk quantification (CRQ) methods and tools, and what are the benefits so far? Discover the challenges and impacts of CRQ adoption identified by technology leaders.

One-Minute Insights:

- Cyber insurance and compliance reporting are the most reported use cases among surveyed leaders
- Over three-quarters of respondents at organizations that have adopted CRQ have increased their investment in it
- Many face challenges related to stakeholder perceptions of CRQ and scoping issues
- Respondents commonly turn to third-party service providers or consultants for CRQ

One-Minute Insights on timely topics are available to Gartner Peer Community members. Sign up for access to over 100 more, and new insights each week.

Data collection: Apr 1 - Jun 28, 2023

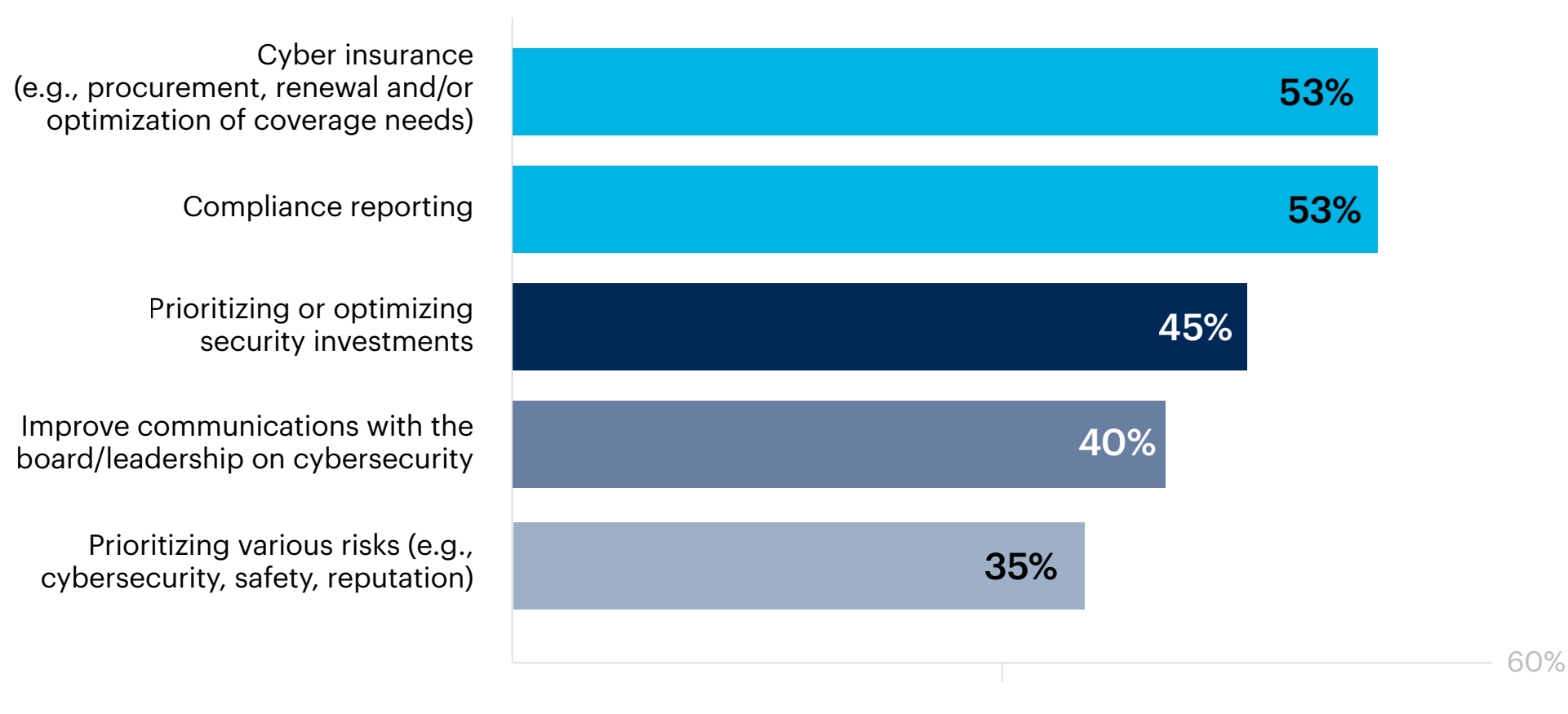
Respondents: 227 IT and information security leaders whose organizations have implemented, are implementing or are planning to implement cyber risk quantification

Most surveyed leaders use CRQ for cyber insurance or compliance purposes

Over half (**53%**) of respondents list **cyber insurance** or **compliance reporting** among their use cases.

Other use cases commonly reported by surveyed leaders include prioritizing or optimizing security spend (45%), improving communications with the board or leadership regarding cybersecurity (40%) and prioritizing different risks (35%).

What are your current or planned use cases for CRQ? Select all that apply.



Security controls (e.g., CRQ used as part of evaluations or exceptions process) **26%** | Evaluating cybersecurity program **22%** | Prioritizing vulnerabilities for remediation **19%** | Demonstrating/articulating ROI of cybersecurity program **14%** | Third-party risk assessment **13%** | Mergers/acquisitions assessments **7%** | None of these **1%** | Not sure **0%** | Other **0%**

n = 227

> "Risk quantification is a must to get executive buy in and endorsement."
>
> - Director, telecommunications industry, 10,000+ employees

> "Early days, we hope to make this a standard way of reporting."
>
> - C-suite, healthcare industry, 1,000 - 5,000 employees

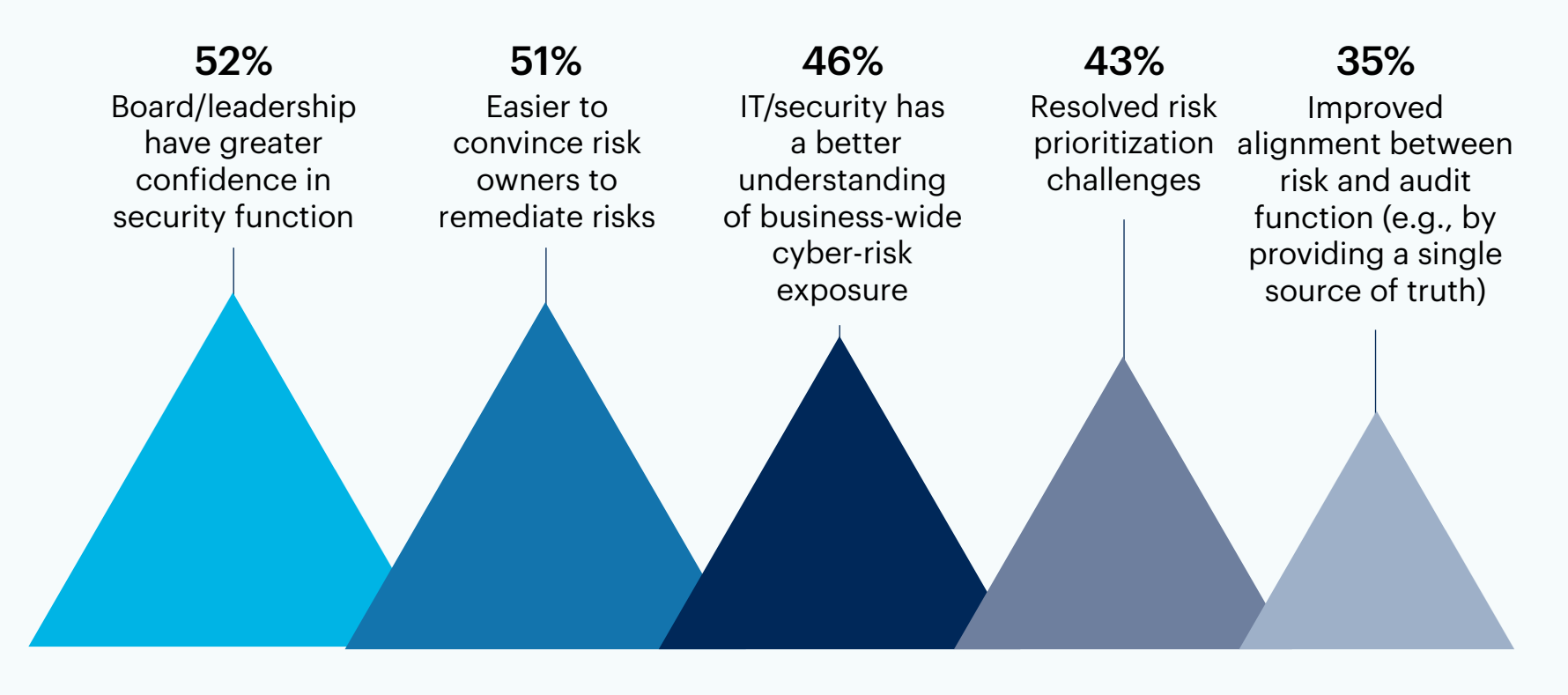
Question: Please share any final thoughts on your organization's experience with CRQ.

Nearly all respondents at organizations that adopted CRQ see beneficial results and many saw increased investments in this area

97% of surveyed leaders whose organizations have adopted CRQ (n = 208) say they **have seen benefits in their organization** as a result.

52% report that **CRQ adoption has given the board/leadership greater confidence** in the security function, and 51% say CRQ has made it easier to get risk owners to conduct remediation. Nearly half (46%) note that CRQ has improved IT/security's understanding of cyber-risk exposure across the business.

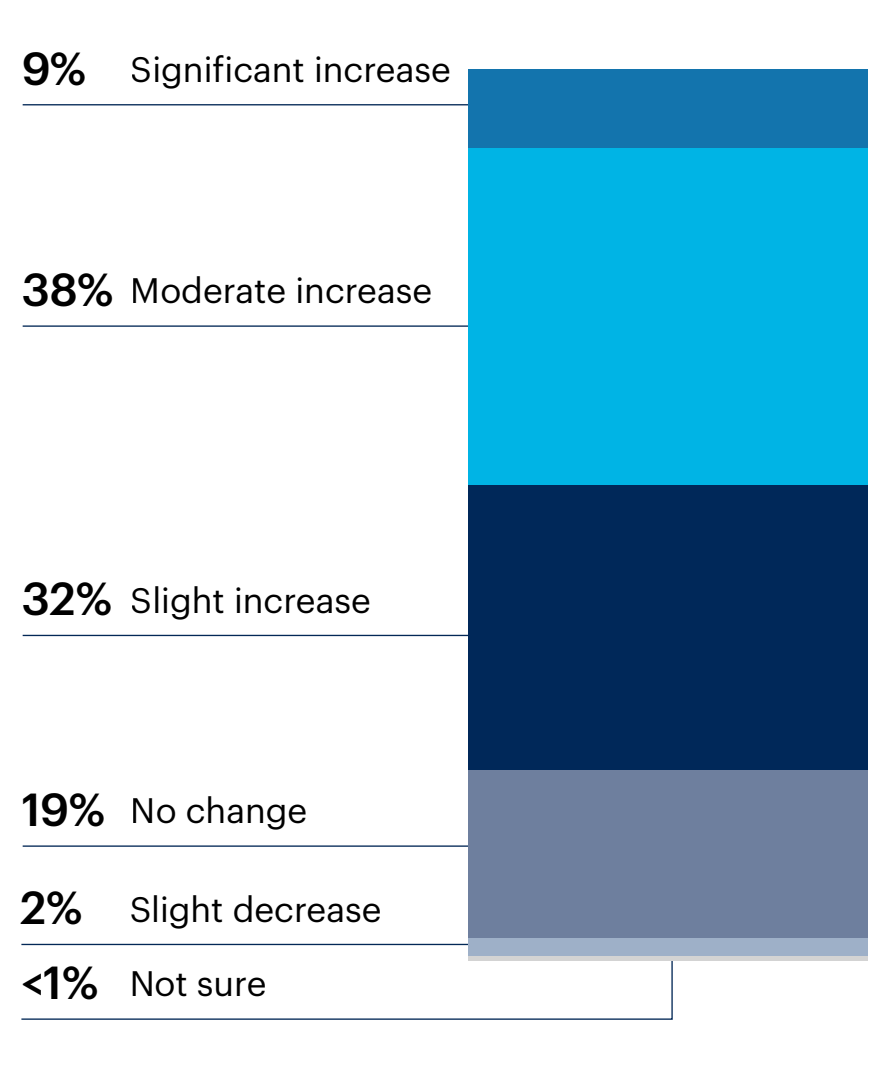
What benefits have you seen in your organization as a result of CRQ? Select all that apply.



Improved communication between security team and other stakeholders (including board and leadership) **27%** | Improved compliance scores **25%** | Improved reporting (e.g., to board, regulators, etc.) **25%** | Improved documentation **13%** | We have not seen any benefits so far **3%** | None of these **1%** | Other **0%**

n = 208

Question shown only to respondents who answered "Yes" to "Has your organization adopted CRQ?"



Among those whose organizations have already adopted it (n = 208), **79%** report that their **investment in CRQ has increased** over the past year.

Has your level of investment in CRQ changed over the past year?

n = 208

Moderate decrease **0%** | Significant decrease **0%**

Question shown only to respondents who answered "Yes" to "Has your organization adopted CRQ?"

> "It requires a lot of effort and collaboration, but it's proving to be worth it."
>
> - VP, retail industry, 1,000 - 5,000 employees

> "Our CRQ implementation has improved cyber risk management, communication with stakeholders, and alignment with business objectives. Continuous monitoring and strategic risk management are key takeaways from our experience with CRQ."
>
> - C-suite, real estate industry, 5,000 - 10,000 employees

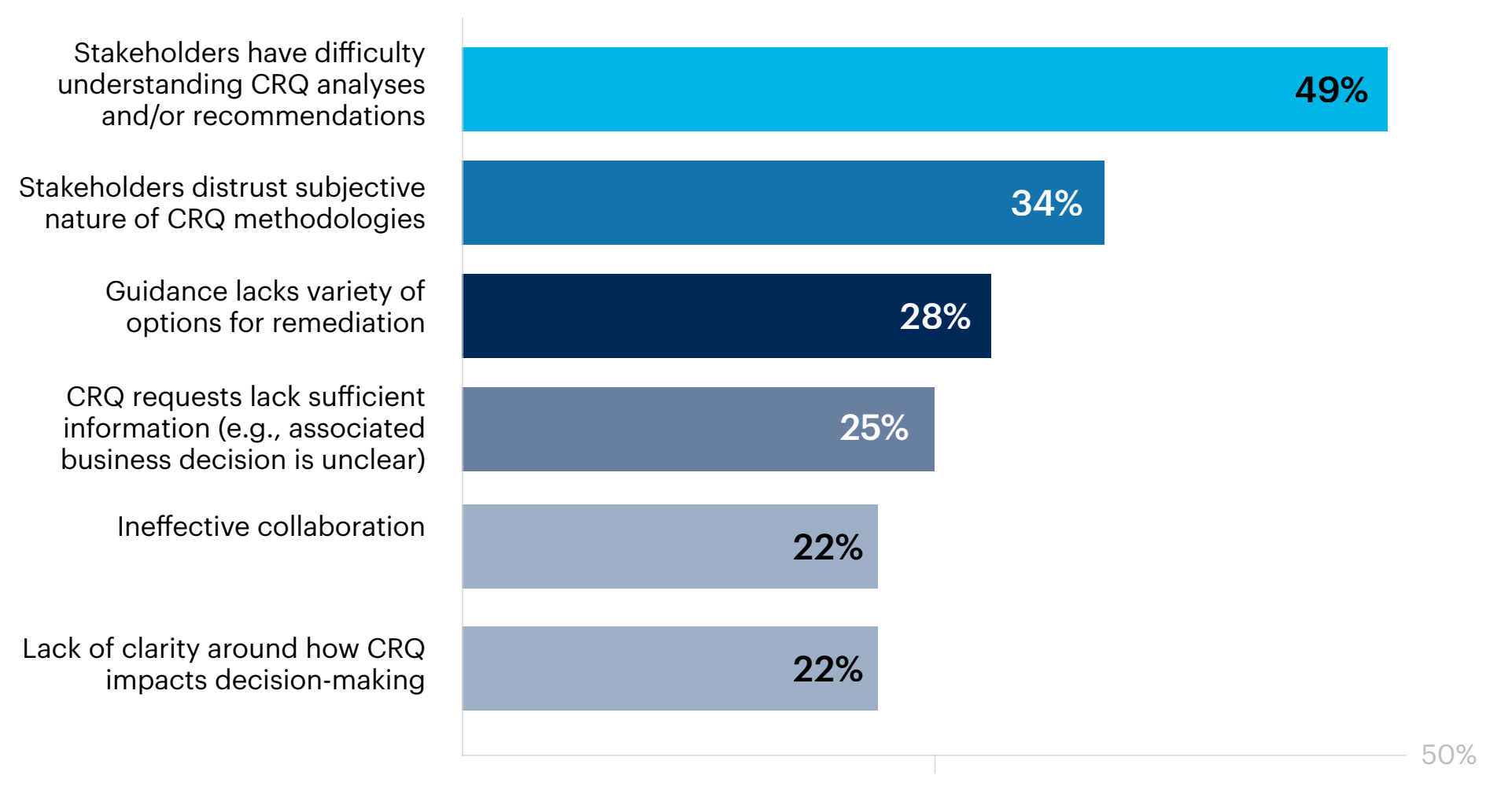
Question: Please share any final thoughts on your organization's experience with CRQ.

Stakeholders struggle to trust or understand CRQ methodologies

The most commonly reported challenge among respondents is that **stakeholders struggle to understand CRQ analyses or recommendations (49%).**

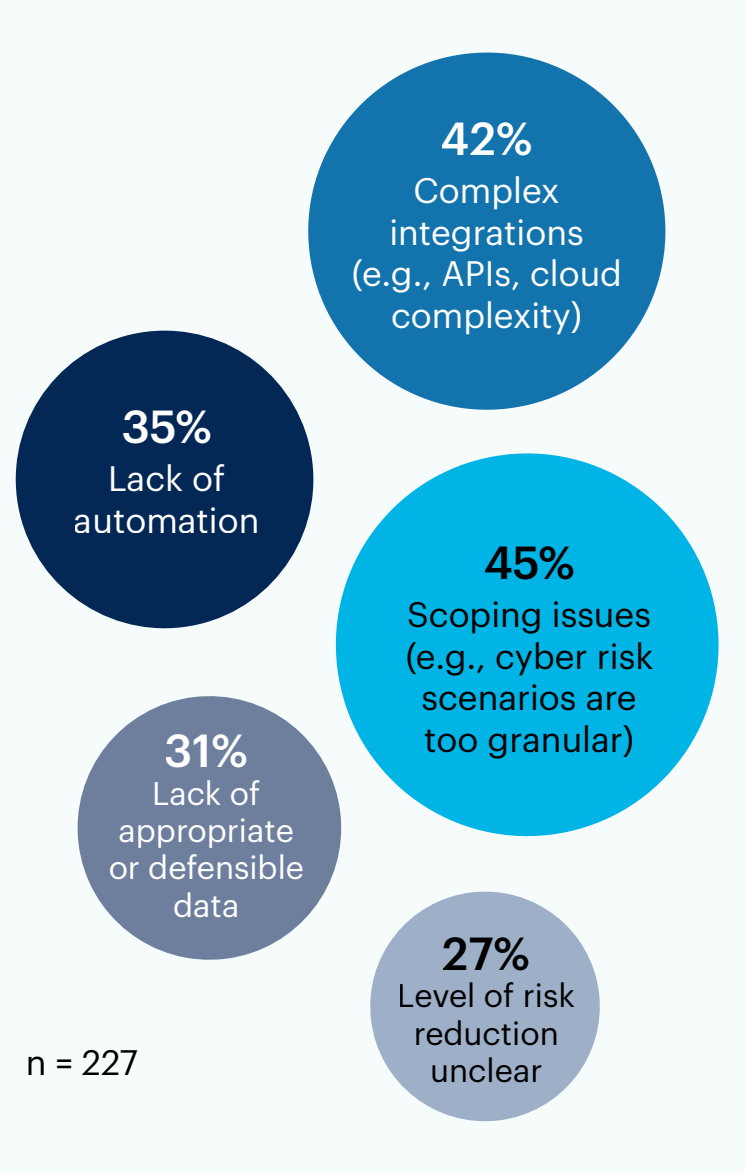
Over one-third (**34%**) of these leaders say **stakeholders distrust the subjective nature of CRQ methodologies** and 28% face difficulties due to a lack of variety in options for remediation.

What organizational or strategic challenges have you experienced with CRQ adoption in your organization? Select all that apply.



Impacts unclear to stakeholders (e.g., risks lack business context in CRQ analyses) **21%** | Team/skills gaps **21%** | Absence of formal CRQ definition **16%** | Time to value is too long **14%** | Executive buy-in **11%** | Costs **11%** | We have not faced organizational or strategic challenges so far **8%** | None of these **1%** | Other **0%**

n = 227



n = 227

Many surveyed leaders face technical challenges with **scoping (45%)** or **integration complexity (42%)**. About one-third note **deficiencies in automation (35%)** or the **availability of appropriate/defensible data (31%).**

What technical challenges have you experienced with CRQ adoption in your organization? Select all that apply.

Delivery of results is not timely enough **26%** | Existing enterprise data underused **26%** | No control catalog available for CRQ **17%** | We have not faced technical challenges so far **8%** | None of these **<1%** | Other* **<1%**

*Other includes: "No clear internal impact data"

> "This is hard without the right internal understanding of potential costs. It is quite subjective."
>
> - C-suite, finance industry, 10,000+ employees

> "Consultants often only consider a limited amount of physical security risks, which may not accurately reflect your operating conditions."
>
> - VP, utilities industry, 1,000 - 5,000 employees

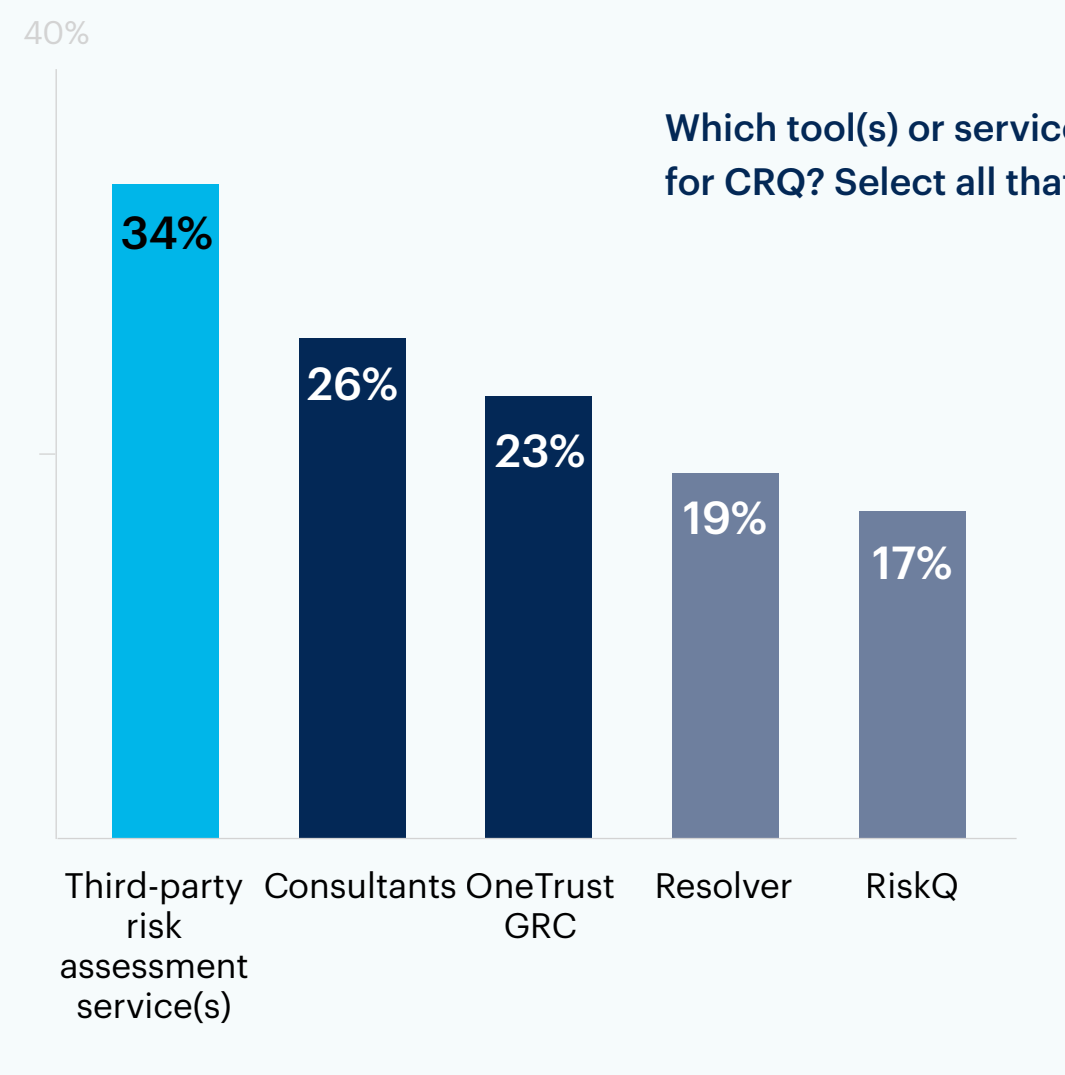
Question: Please share any final thoughts on your organization's experience with CRQ.

Use of third-party services or consultants for CRQ is common, and most strategies include post-assessment impact analysis

34% of respondents are using **third-party risk assessment services** for CRQ and nearly one-third (**26%**) are working with **consultants** for this purpose.

The CRQ tools most commonly listed by surveyed leaders are **OneTrust GRC (23%)**, **Resolver (19%)** and **RiskQ (17%).**

Which tool(s) or services are you using or planning to use for CRQ? Select all that apply.



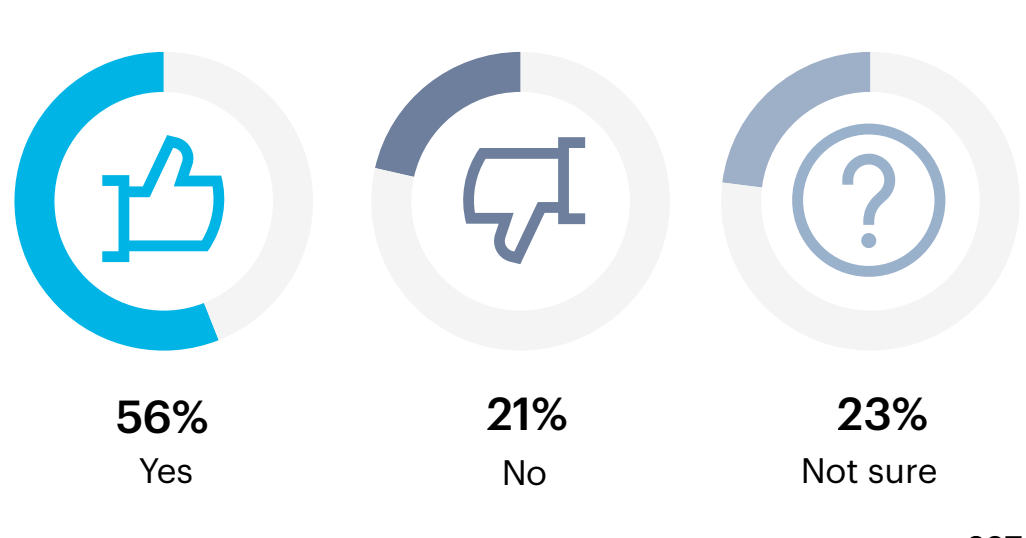
Arx Nimbus **16%** | RiskLens **13%** | ThreatConnect **11%** | VisibleRisk **10%** | MetricStream **9%** | Acuity Risk Management **9%** | None of these **7%** | Kovrr Quantum **6%** | Axio **6%** | Balbix **5%** | Not sure **4%** | Other* **2%**

n = 227

*Other includes: "In house analytics", "Internal research"

Over half (**56%**) say their organization's strategy does or will include a **screening process to identify which business decisions require CRQ** assessments.

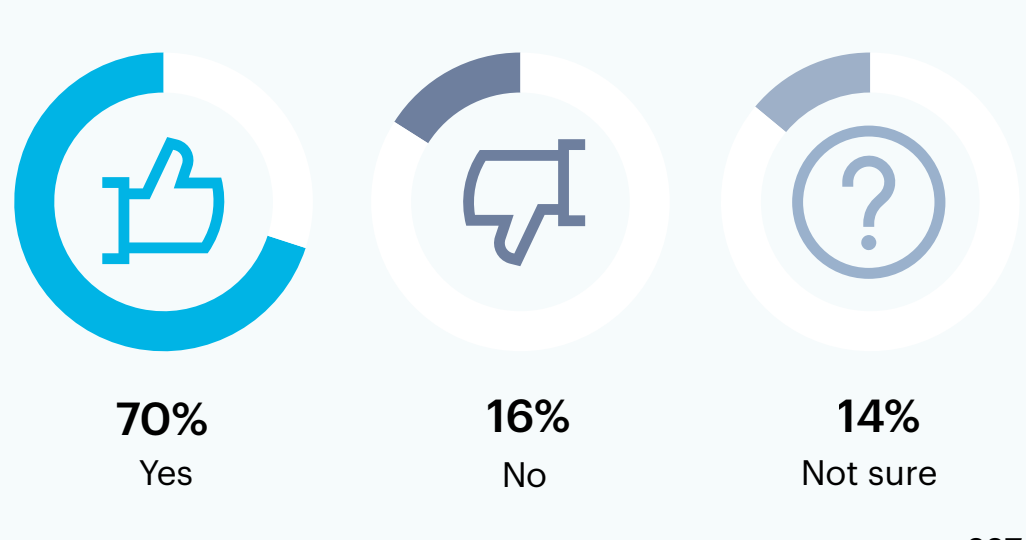
Do you have or plan to implement a screening process to determine which business decisions require CRQ?



n = 227

And almost three-quarters (**70%**) say their organization does or will have a **post-assessment process to evaluate CRQ's impact** on business decisions.

Do you have or plan to implement a post-assessment process to evaluate if and how CRQ analyses impact business decisions?



n = 227

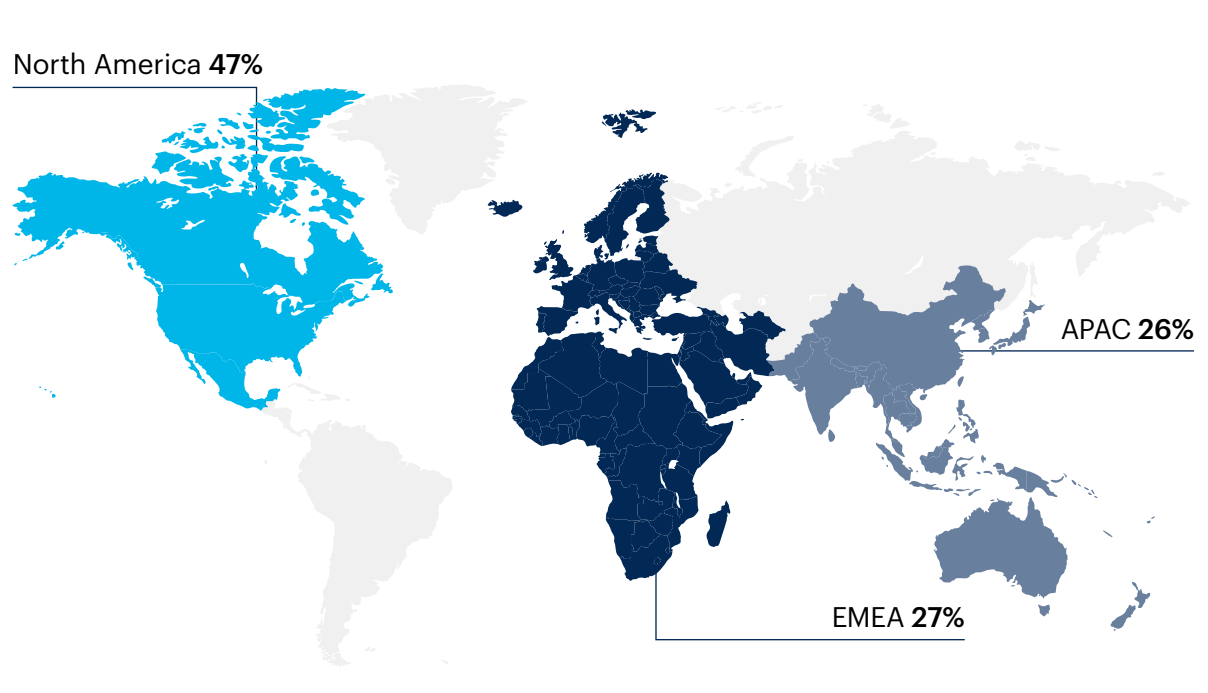
> "It has to be implemented in a phased manner. A POC is important after the initial study so that an impact in the area can be demonstrated."
>
> - C-suite, utilities industry, 10,000+ employees

> "We've performed CRQ internally and then brought in an external firm to assist with our own. We found outsourcing to be much more effective in driving to value and deadlines. You should definitely do some analysis on the tooling that the company is using as well as the methodology they've implemented which leads them to the recommendations they provide you. Tools are easy to use — but experience is what leads to better recommendations."
>
> - C-suite, software industry, 10,000+ employees

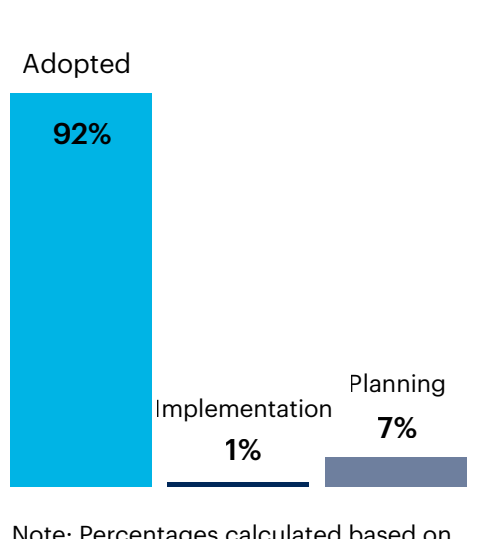
Question: Please share any final thoughts on your organization's experience with CRQ.

Respondent Breakdown

Region

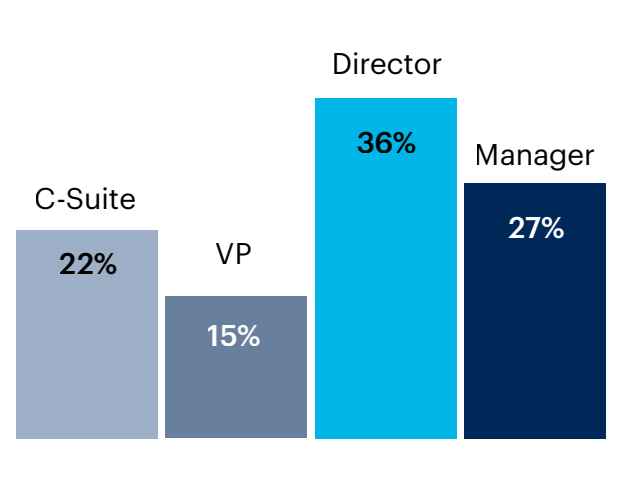


Respondent Organizations CRQ Adoption Stage

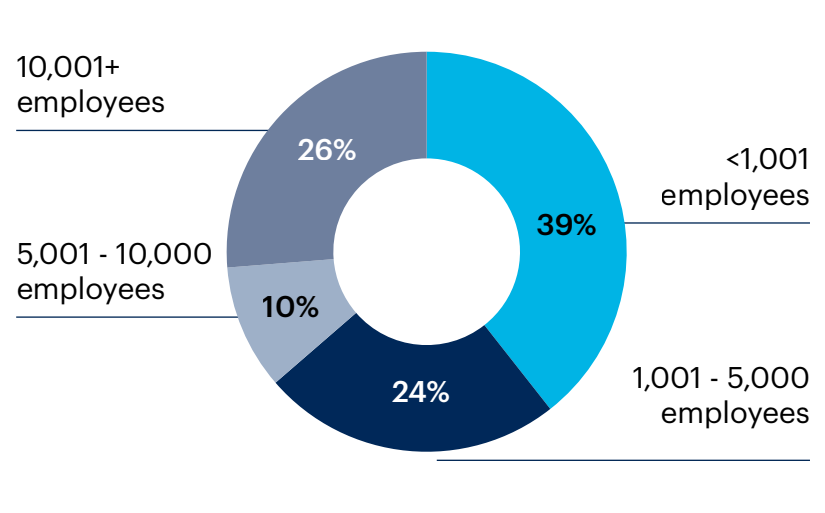


Note: Percentages calculated based on responses to "Has your organization adopted CRQ?" and "Is your organization planning to adopt CRQ?".

Job Level



Company Size



Note: May not add up to 100% due to rounding

Respondents: 227 IT and information security leaders whose organizations have implemented, are implementing or are planning to implement cyber risk quantification

Gartner

Source: Gartner Peer Community, Cyber Risk Quantification (CRQ): Adoption and Impacts survey