



KPMG Enterprise Risk & Resiliency Survey

C-Suite Insights

Results

—

March 2025

Key Findings – Risk and Resilience Operating Models

Risk and Resiliency Management Structure

- **Strategic Risk & Resiliency Integration:** Two-thirds of organizations have integrated risk and resilience into their business strategy and planning (64%). Resilience (58%) is less integrated than risk management (64%) into individual business function planning.
- **Centralization and Coordination:** Half of companies have centralized or coordinated structures for managing risk and resiliency (48%).
- **Organizations with centralized risk and resiliency management structures perform better across the board:** Including fewer barriers to managing risk, more focus on tracking emerging risks, mature integration, and stronger confidence that their C-suite understands business risks.
- **Public and Private organizations have more similarities than differences:** These organizations are similar in terms of risk and resiliency management approach, maturity of developing strategy, integrating processes, and leveraging technology, data/analytics and reporting.

Risk Operating Model

- **Documentation vs. Application:** Organizations are further along in ‘completely’ documenting risk guidelines (48%) and procedures (47%) than they are with their risk strategy documentation (38%). And while many organizations have ‘completely’ or ‘mostly’ documented risk strategies, guidelines and procedures, around half are only ‘somewhat consistent’ in the application of these strategies.
- **Risk Management barriers:** Two-thirds to nearly three-quarters of organizations face moderate or strong barriers to effectively managing risk.
- **Cybersecurity & ERM:** It is more common (50%) to have periodic/report driven integration of cybersecurity and ERM programs; a third (32%) have achieved mature integration between these two areas.

Key Findings – Risk and Resilience Operating Models

Resiliency Operating Model

- **Risk Area Improvement:** The biggest risk areas (cybersecurity, data privacy, technology, environmental and financial) are also described as top areas to address with improved resiliency planning and procedures.
- **Implementing Resiliency Planning and Procedures:** Half of the organizations have fully implemented resiliency plans for critical processes. However, only 17% have extended these plans beyond critical processes, and 44% have plans with mixed product/geographical coverage or limited critical process coverage. The limited expansion of resiliency plans beyond critical processes suggested that many organizations are not fully prepared to handle broader disruptions.
- **Testing and Updating Resiliency Plans:** Most organizations (51%) test and update their resiliency plans annually, while a quarter (23%) are doing so more than once a year.
- **Use of Risk Assessments:** 7 in 10 (69%) organizations are leveraging enterprise risk assessment results to inform their resiliency strategy and investments. A smaller portion (24%) are relying on business impact analysis and IT risk assessments, and only 7% do not use any risk assessments.
- **Leadership and Accountability:** Around three-quarters (72%) of organizations have senior leadership accountable for enterprise resiliency. However, resiliency responsibility is spread across roles – a third (35%) of organizations have appointed a Chief Risk Officer (CRO), but this responsibility also falls under other C-Suite roles (CIOs, COOs, or CTOs).
- **Confidence in C-Suite Understanding:** 41% of organizations are strongly confident that their C-suite recognizes the business risks associated with a critical process outage or failure, while 52% are somewhat confident.

Key Findings – Risk and Resilience Operating Models

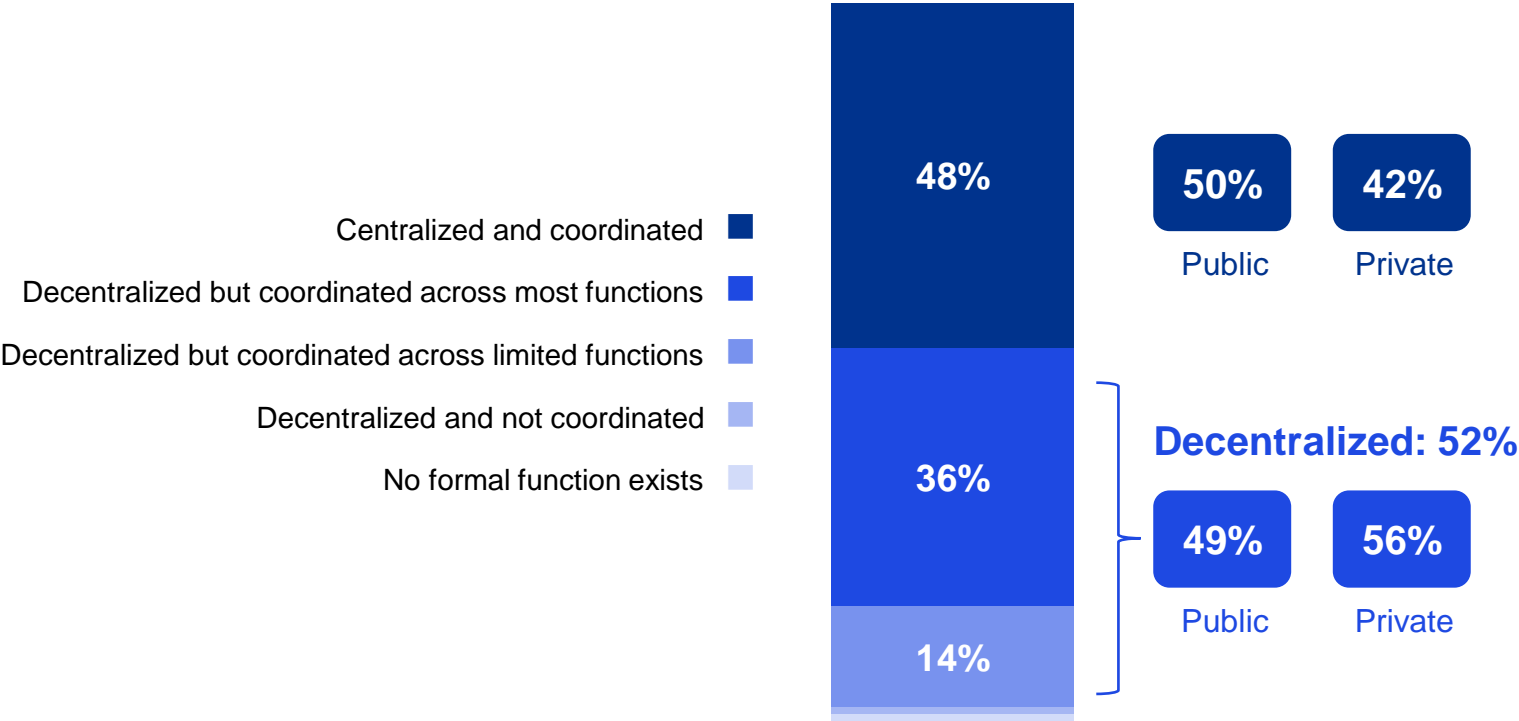
Technology, Data, Analytics & Reporting

- **Technology Utilization:** The use of specialized tools (i.e., GRC technologies, risk monitoring tools, risk reporting technologies) is common with two-thirds relying on them to manage all (18%) or nearly all (50%) of their risk processes to identify, assess, track, and mitigate risks.
- **Risk Process Automation:** Two-thirds (65%) have mostly automated their risk management processes, but few (11%) have automated it fully. Public companies have reached higher levels of automation with three-fourths (72%) mostly automated – compared to just over half (54%) of private companies.
- **Advanced Analytics:** Half of organizations regularly rely on advanced analytics (50%), with only about one in seven heavily relying on it (15%). About three in ten (29%) use advanced analytics on an ad-hoc basis.
- **Risk Reporting Data Quality and Accessibility:** Organizations describe their risk reporting data as high quality (32%) or mostly complete (56%) – and fully (38%) or mostly (42%) accessible.
- **Risk Reporting Data Integration:** A quarter (24%) have fully integrated risk reporting data and half (50%) have it mostly integrated.
- **Timeliness of Risk Reporting Data:** Data used in risk reporting is described as very or mostly timely by nearly all organizations (88%).
- **Use of External Data Sources:** Two-thirds (68%) of organizations are always or often leveraging external data sources, such as market trends and industry benchmarks, to enhance their risk analysis.

Almost half (48%) of companies have a centralized structure for managing risk and resilience functions.

Just over one-third (36%) are decentralized but are coordinating most of their risk and resilience functions.

Organization Structure for Managing Risk and Resilience



Centralized & decentralized risk and resiliency organizations are proportionate to each other in terms of company size, industry and representation across public and private companies.

Q2. How would you describe your organization's structure for managing Risk and Resilience? (n=208) | Public (n=137), Private (n=71)

Cybersecurity is expected to be the biggest risk area for businesses over the next 5 years.

Private companies are also concerned with data privacy risk and environmental risk is the next biggest concern (after Cyber) for Public companies.

Biggest Risks Organization will Face over the next 2-5 years

Select up to 7 risks

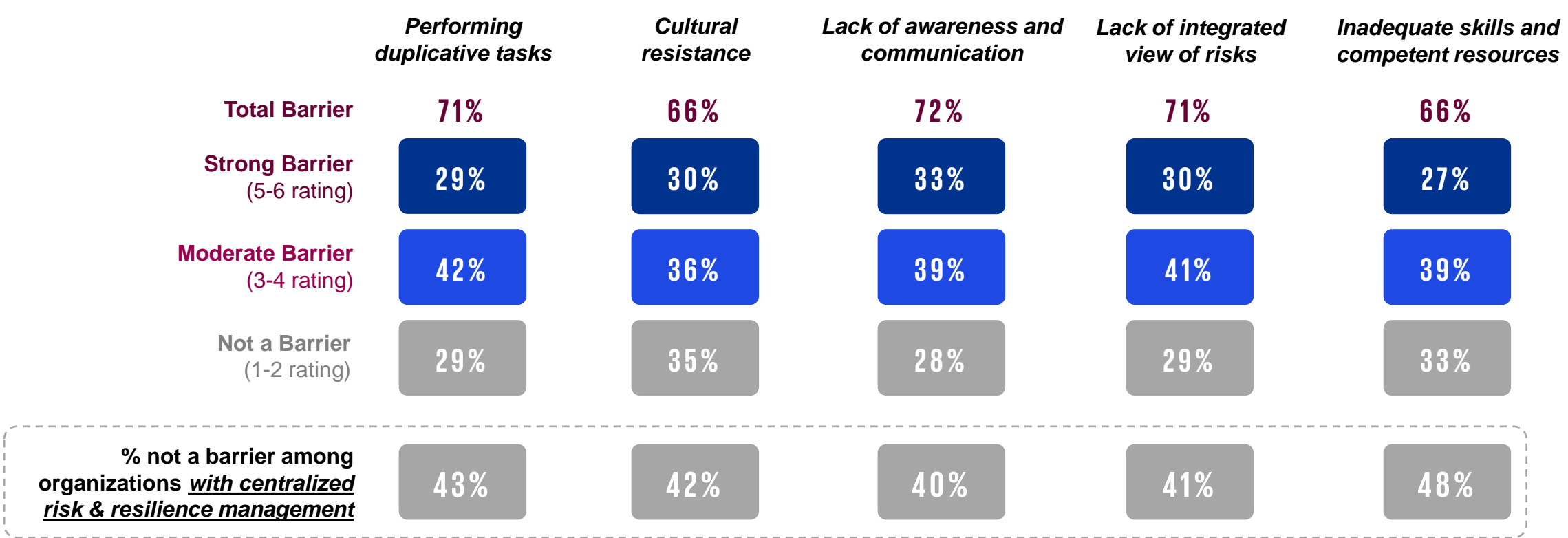


Q1. What do you think are the biggest risks your organization will face within the next 2-5 years? (n=208) | Public (n=137), Private (n=71)

Two-thirds or more of organizations face moderate to strong barriers when managing risk.

However, organizations with centralized risk and resilience management structures are less likely to cite any risk management barriers.

Barriers to effectively managing risk at organization

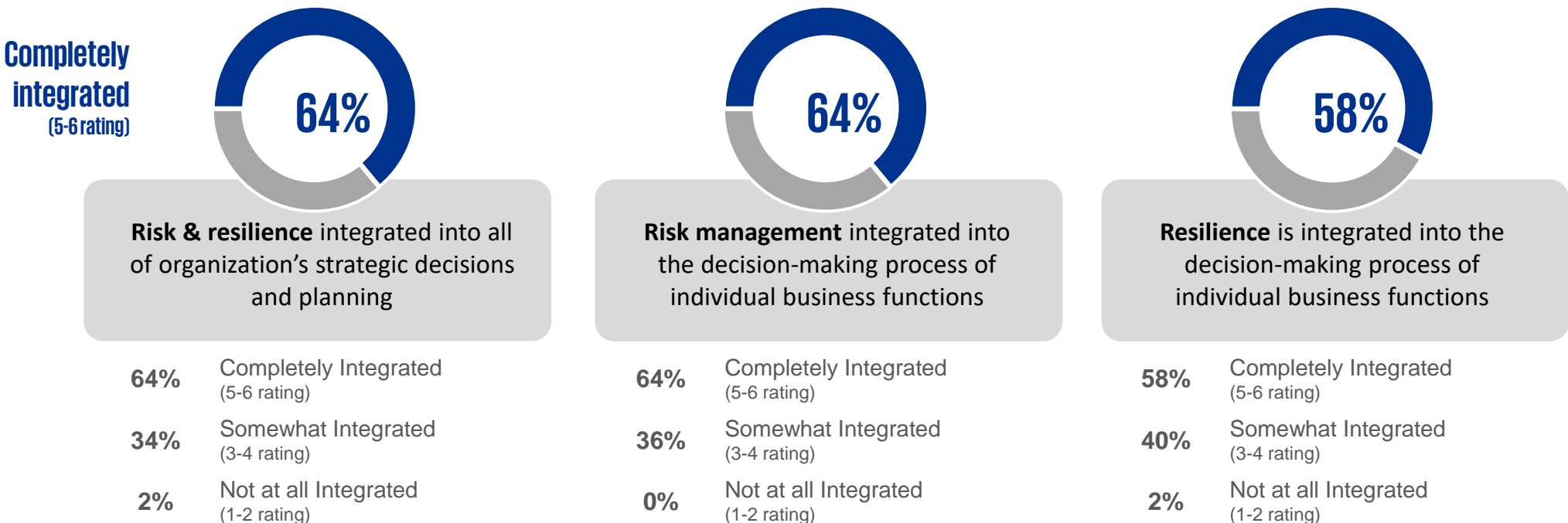


Q10. Please rate the degree to which each of the following are barriers to effectively managing risk at your organization. (n=208)

Two-thirds of companies have integrated risk and resilience into overall strategy and planning decisions.

Resilience (58%) trails behind risk management (64%) when it comes to being fully integrated with individual business function planning.

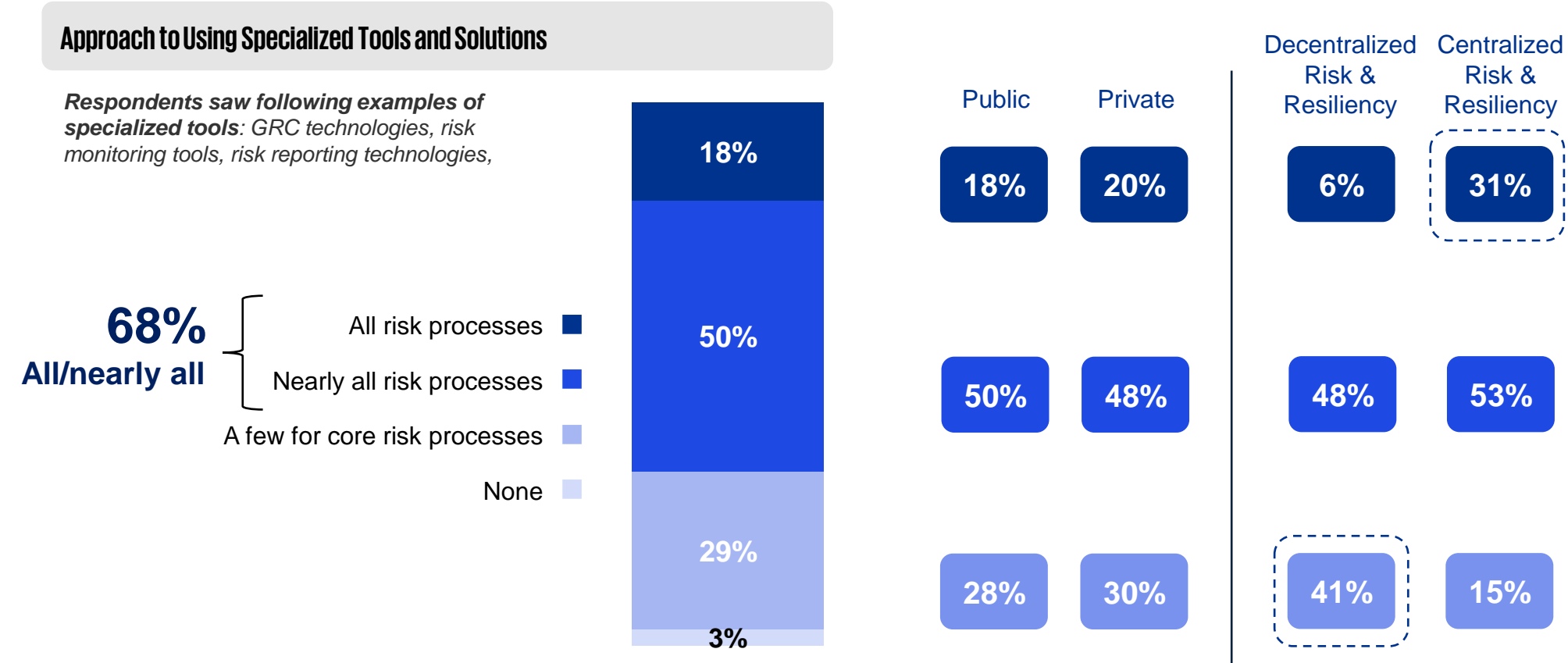
Integration of Risk and Resilience Management into strategic planning and business functions



Q4. To what extent is risk and resilience management integrated into all your organization's strategic decisions and planning? | Q5. To what extent is risk management integrated into the decision-making process of individual business functions (sales, marketing, supply chain, finance, IT, operations, etc.) at your organization? | Q6. To what extent is resilience integrated into the decision-making process of individual business functions (sales, marketing, supply chain, finance, IT, operations, etc.) at your organization? (n=208)

Two-thirds (68%) of companies utilize special tools and solutions for nearly all if not all risk processes.

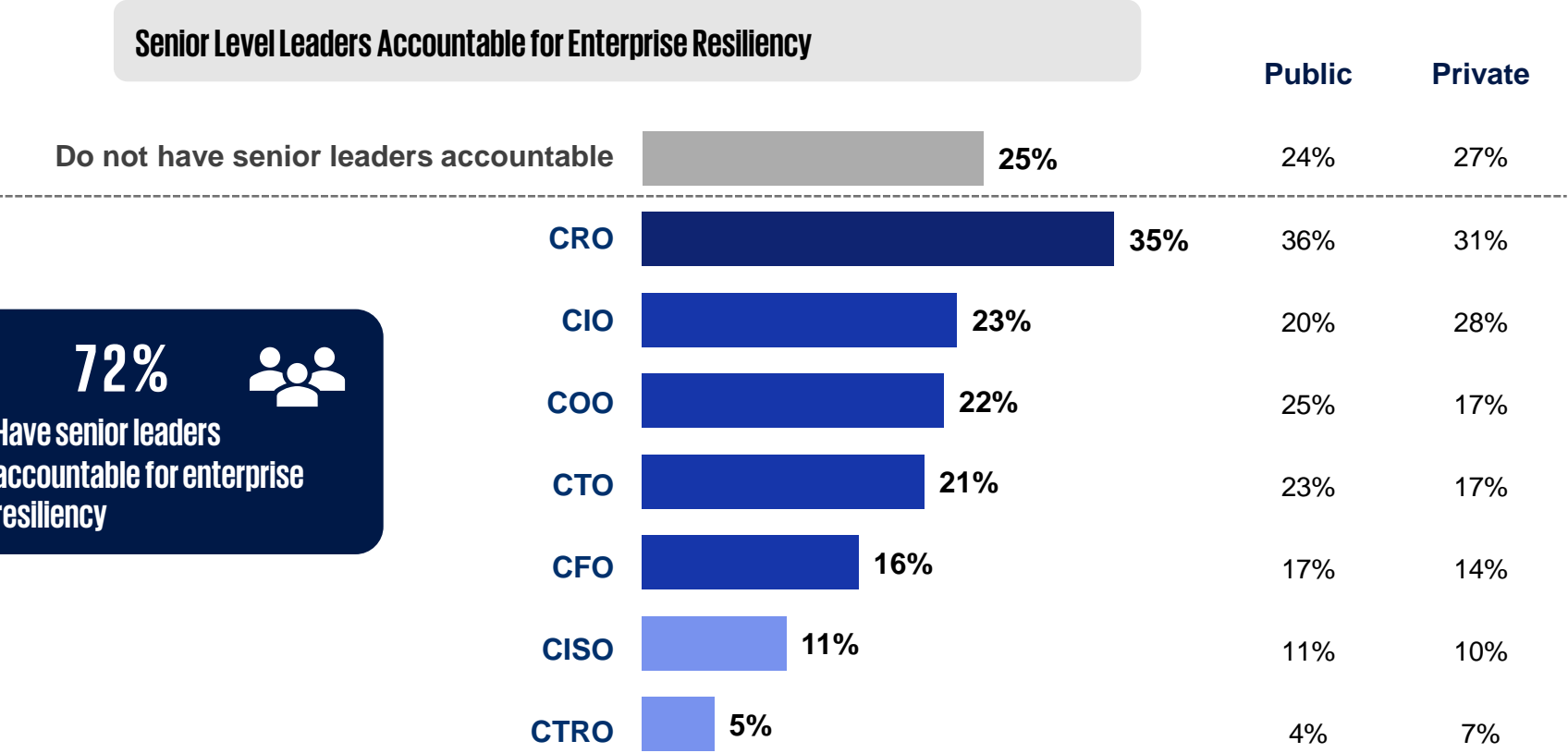
Those with centralized risk and resiliency are using specialized tools for all risk processes much more frequently than those with decentralized structures.



Q23. Which of the following best describes your current approach to using specific tools and solutions to help you identify, assess, track, and mitigate risks? For example, GRC technologies, risk monitoring tools, risk reporting technologies, etc. Select one. (n=208) | Public (n=137), Private (n=71) | Decentralized (n=107), Centralized (n=99)

About three-quarters (72%) of organizations have senior leadership accountable for enterprise resiliency.

A third (35%) of organizations have appointed a Chief Risk Officer (CRO); nearly 1 in 5 (~20%) organizations task their CIOs, COOs and CTOs with this responsibility. 6 in 10 (58%) organizations have 1-2 resiliency leaders.



72%

Have senior leaders accountable for enterprise resiliency

of Senior Resiliency Leaders

31%
1 Senior Leader (n=64)

27%
2 Senior Leaders (n=56)

14%
3+ Senior Leaders (n=29)

25%
No senior leader (n=59)

Q17. Do you currently have a senior level leader(s), with a supporting team, accountable for enterprise resiliency? (n=208) | Q17.1 Who? Select all that apply. (Rebase: n=208) | | Public (Rebase: n=137), Private (Rebase: n=71)