READINESS REPORT

kyndryl

Executive Summary Report



2026-27

AI returns rise while readiness falls

In this year's Kyndryl Readiness Report, more business and technology leaders reported that AI is delivering value to their organizations: Among organizations investing in AI and machine learning, 64% of them say it's delivered positive returns. That is up from 42% who agreed in 2024 and 54% in 2025. Leaders are no longer waiting for AI to prove its value.

At the same time, leaders report a drop in confidence. On average, only 24% of leaders say their organizations are completely ready to manage external risks: a seven-point drop from 2025. For the third year in a row, cyberattacks topped the list of external concerns, and readiness for them dropped 11 points. Organizations are discovering that successful AI deployment brings a new set of challenges and demands.

This year's findings highlight an evolution in how organizations think about integrating AI into their work, the technology needed to support it and the risks they must manage. As AI moves deeper into the business, the bar for readiness moves with it. Nearly half (48%) significantly changed their AI strategy in the past year, and 59% feel more pressure than they did 12 months ago to prove ROI on their agentic AI investments.

Organizations made progress adopting AI and are moving beyond the pilot phase. Fewer leaders describe themselves as in the AI experimentation phase (49%, down from 62% last year), and 84% have deployed AI in workflows beyond pilots.

Organizations, then, have AI deployed in some production workflows while still describing their broader adoption as experimental. Fewer leaders also say innovation stalls after proof of concept (45%, down from 57%). Yet these numbers are still high, and progress in one area has not closed the readiness gap across others.

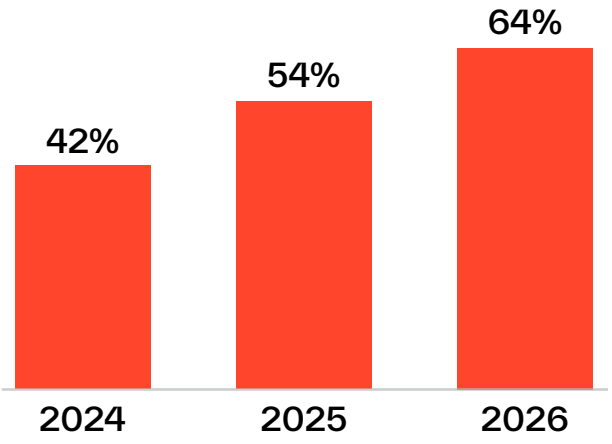
Leaders are saying they need a more deliberate way to decide which projects deserve funding and what has to change around them. Thirty-eight percent say modernization decisions are not consistently tied to business strategy; another 38% say their AI strategy emerged by accident rather than design. Nearly four in ten (39%) have seen an investment fail or have canceled a major initiative, and 59% say short-term ROI pressure undermines longer-term innovation goals. These findings point to a challenge that extends beyond technology adoption.

Continuous readiness demands investment across three dimensions: Foundation, Reinvention and Control. The defining question for 2027 is whether an enterprise can continuously transform and accelerate value without sacrificing resilience.

AI returns rise while readiness falls

More firms are reporting positive ROI in their AI and machine learning investments

Positive ROI - AI and machine learning

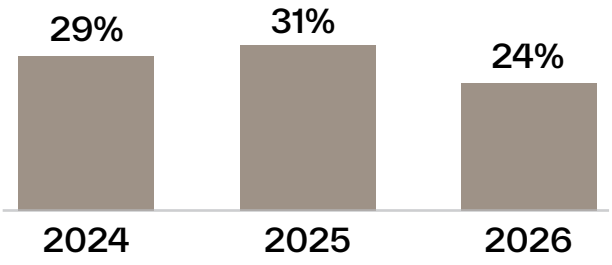


+22 pts since 2024

+10 pts since 2025

While the average share of leaders reporting complete preparedness for external risks fell 7 points

Average readiness across external risks



-5 pts since 2024

-7 pts since 2025

Q33: Thinking about the specific digital technologies, tools or solutions your organization is currently investing in, how would you describe the return on investment (ROI) your company has experienced as a result of these investments? Q16. How ready would you say your organization currently is to manage the following external business risks? Base: Total (n=3700).

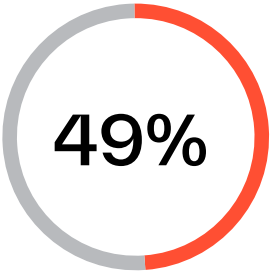
Leaders see the race for pilots wane as focus turns to repeatable value



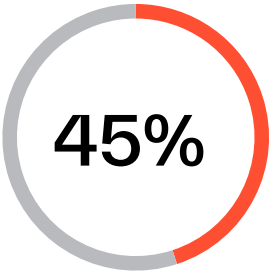
84%

of organizations report they are deploying AI in workflows beyond pilot projects

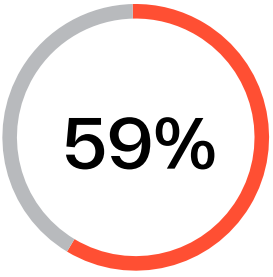
Agreement about my organization's adoption of emerging technology
% Agree



describe their organizations as in the experimentation phase when it comes to AI, **down 13 pts since 2025**



report innovation efforts often stall after the proof-of-concept phase, **down 12 pts from 2025**

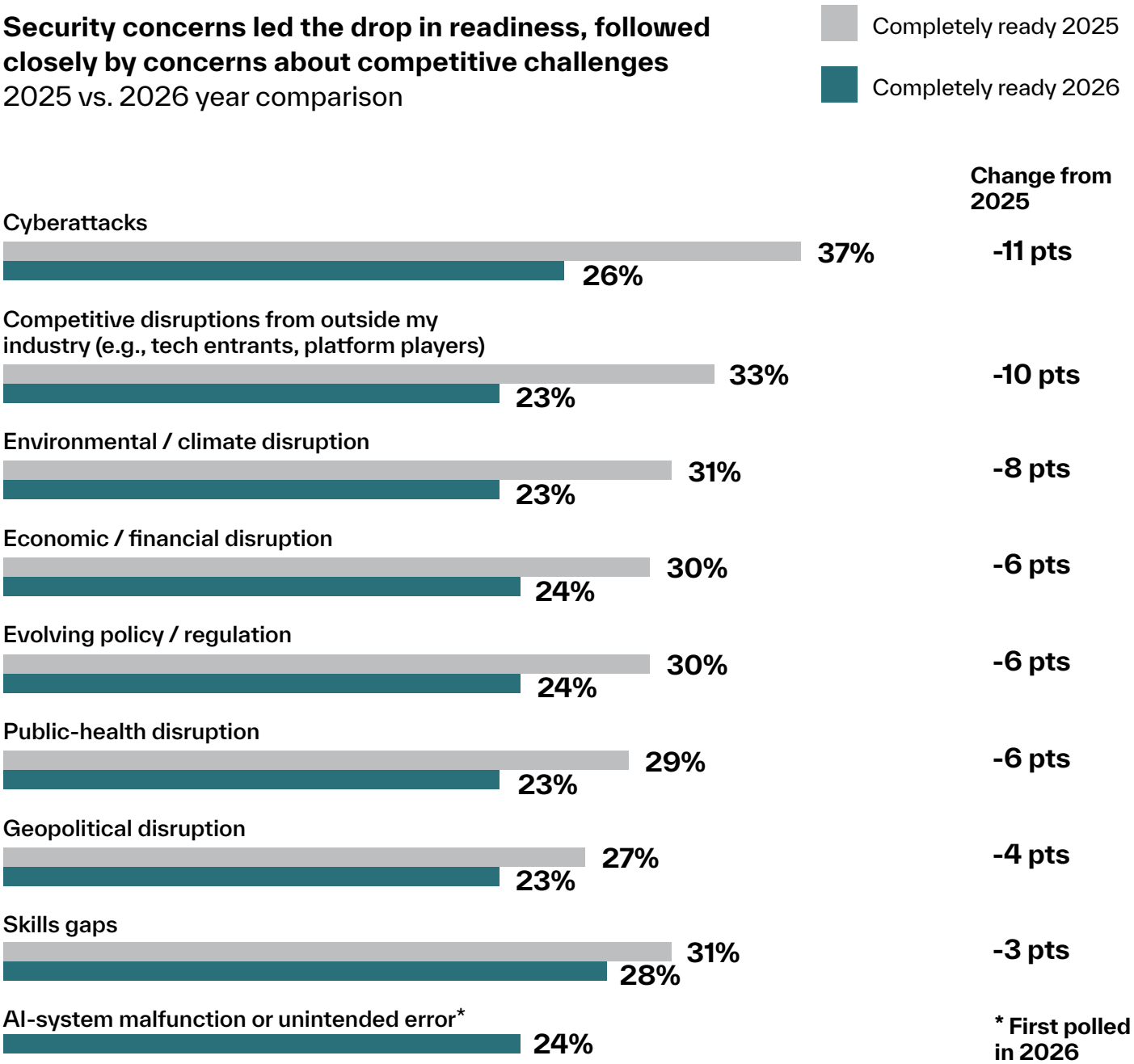


feel more pressure than 12 months ago to **prove agentic AI ROI**

Q8: How much do you agree or disagree with the following statements about your organization's adoption of emerging technologies?
Base: Total (n=3700)

Compared to one year ago, substantially fewer leaders report they are completely ready across a range of external risks

Security concerns led the drop in readiness, followed closely by concerns about competitive challenges
2025 vs. 2026 year comparison



Q16: How ready would you say your organization currently is to manage the following external business risks? Base: Total (n=3700)

Three dimensions of readiness increasingly matter together: technology foundations, capacity for reinvention, and maintaining control

Technology will not stop moving long enough for an enterprise to become permanently ready. Organizations need to manage three dimensions at once: continuously evolve the technology foundation, reinvent how work gets done and maintain control as environments become more complex. Together, these define continuous readiness — the ability to translate technological change into business value repeatedly, without sacrificing resilience or strategic alignment.

Foundation

Can the technology estate evolve as AI, business and sovereignty requirements change?

Reinvention

Can organizations redesign workflows, roles and measures as AI changes how work gets done?

Control

Can leaders maintain visibility, accountability and resilience as complexity and risk exposure grow?

Foundation: Why leaders say a modern foundation isn't the same as one ready for AI

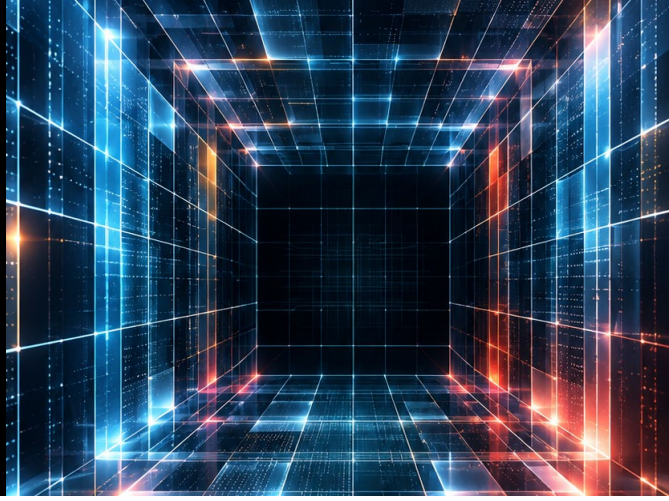
AI is asking more of foundations leaders already consider modern

Most leaders consider their core IT estate modern: 71% say it is mostly or fully modernized. Yet 62% say their foundation needs further modernization before they can fully realize AI's benefits, and 58% of all leaders (and two-thirds of CIOs) say it needs significant re-architecture to support AI at scale. The data points to two problems.

The first is data. Four in ten say their data is not ready to support AI at scale, and 46% say data silos limit their ability to scale AI initiatives. The second is what earlier modernization left behind. Cloud increased agility for 86%, but 60% experienced higher-than-expected costs, 48% say their environment evolved by accident rather than design, and 48% have data stranded in environments that were never decommissioned. Complete readiness also fell this year across infrastructure, networks, cloud and data centers.

Where these problems are addressed, the returns show. Organizations that avoided cloud setbacks report positive AI/ML returns at 73% vs. 58%, those with a mostly or fully modernized estate at 67% vs. 56%, and those whose data isn't ready report an AI investment failure at twice the rate of those whose data is (35% vs. 17%).

Leaders report their IT estates are highly modernized. But AI is raising the requirements for what their technology foundation needs to support.

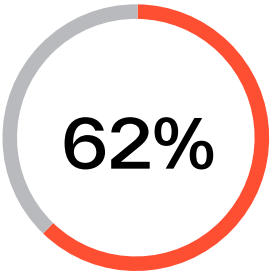


71% of leaders describe their organization's core IT estate as mostly or fully modernized

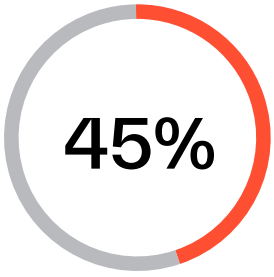
Q1: Which statement best describes the current state of your organization's core IT estate? Base: Total (n=3700)

Perceptions of technology foundation

% Agree



agree their organization needs to modernize its technology foundation before it can fully realize the benefits of AI



agree innovation efforts are often delayed by foundational issues in their technology stack

Q21: How much do you agree or disagree with the following statements? Base: Total (n=3700)



agree their technology foundation requires significant re-architecture before it can support AI at scale

"Individual new technologies are relatively easy to handle, but systemic technological shifts that span the entire company are where most organizations are least prepared."

— Director, Healthcare, Italy



AI demands more from a modernized IT estate

Organizations looking to scale AI should start with what AI will require of the business: the data it needs, the workflows it will support and the infrastructure required to run it at scale.

The question isn't simply whether systems have been upgraded, but whether they can support what the business wants to do with new technologies. That means addressing data quality, access and integration alongside infrastructure, and not assuming a modern estate has already solved them. Those requirements should shape modernization agendas from the outset.

71%

of leaders say their organization's IT estate is mostly or fully modernized

Yet

66%

of CIOs say their technology foundation requires significant re-architecture before it can support AI at scale

and

40%

of leaders say their organization's data is not ready to support AI at scale

AI-ready data:

Among organizations currently investing in AI and machine learning, those whose data is ready for AI at scale:

+16 pts

more likely to report positive returns on their AI and machine learning investments, vs. those whose data is not ready (70% vs. 54%)

No cloud challenges:

Those not experiencing cost, design or data-access setbacks:

+15 pts

more likely to report positive returns on their AI and machine learning investments, compared to those experiencing multiple cost, design or data-access setbacks (73% vs. 58%)

Modernized estates:

Of those with mostly or fully modernized estates:

+11 pts

more likely to report positive returns on their AI and machine learning investments, vs. those with partially or mostly legacy estates (67% vs. 56%)

+14 pts

more likely to report being completely ready to manage future risks affecting their IT infrastructure (37% to 23%)

Reinvention



AI is changing workflows faster than organizations are redesigning work

This year's data shows that organizations have incorporated AI into workflows, and organizations are taking actions to make their investments pay off.

As AI changes how work gets done, the organizational design around it must change too. Seventy-seven percent of leaders say AI agents already automate workflows that once required handoffs between teams or systems. Most report that the work of adapting is under way: 75% agree that roles have been redesigned around AI, and 78% agree that formal change management is in place. Far fewer describe it as finished: only 29% completely agree that change management is fully implemented, and 33% completely agree that their workforce is completely ready to leverage AI.

Three-quarters of leaders prefer to embed AI where ROI is clearest or use it as a productivity layer for their existing work. A small number, 13%, opt to rebuild their core processes and operating models around it.

The data also shows that intentional organizational redesign can deliver value. Among the 65% of organizations that agree both that roles have been redesigned around AI and that formal change management is in place, 69% report positive ROI on AI/ML, compared with 53% of all other organizations. The pattern holds for generative AI (64% vs. 49%) and for agentic AI (59% vs. 49%), meaning redesign is associated with value.



To break innovation stalemates, expand the definition of a pilot

A technology pilot shouldn't merely prove that the technology works. It should be a miniature version of the eventual entire transformation — workflow, roles, adoption and governance — not just the technology.

Organizations tend to build new tools and assume they'll figure out how people work with it afterward. Questions like what the agent does versus the human, who is accountable, and how workflows change need to be addressed during solution design, not handed to change management after deployment.

Most are deploying AI

84%

are deploying AI in workflows beyond pilot projects

Yet deployment precedes transformation

29%

completely agree that formal AI change-management programs are fully implemented across their organizations

45%

say innovation often stalls after proof of concept

Redesigned roles and change management:

Leaders who report their organization has fully redesigned roles and fully implemented change management programs say:

+28 pts

more likely to say their AI implementation is completely ready, compared to those who do not (53% vs. 25%)

+8 pts

more likely to be seeing positive ROI from AI/ML investments, compared to those who do not (71% vs. 63%)

Q6: How much do you agree or disagree with the following statements about your organization's current workforce? Q8: How much do you agree or disagree with the following statements about your organization's adoption of emerging technologies? Q18: How ready would you say these elements of your organization's IT currently are to manage future risks and disruptive forces? Q33: Thinking about the specific digital technologies, tools, or solutions your organization is currently investing in, how would you describe the return on investment (ROI) your company has experienced as a result of these investments? Base: Total (n=3,700), except positive ROI, which is based on respondents investing in AI/ML.

Control



Maintaining visibility and control becomes more critical as technology becomes more interconnected

For the third year in a row, cyberattacks are the leading external concern for business leaders. Just 26% say they are completely ready to manage them (down 11 points year over year).

As AI raises the sophistication, speed and frequency of threats, the technology can also be deployed for greater defensive capabilities. Yet at the current moment, more leaders express concern about increased threats than confidence about their organizations' ability to defend against them. Organizations depend on a wider network of third parties, data environments and technology providers. As AI becomes more embedded in IT operations and cybersecurity, organizations need visibility into how systems are used, where accountability sits, which third parties they rely on and how fast they can respond when risks emerge.

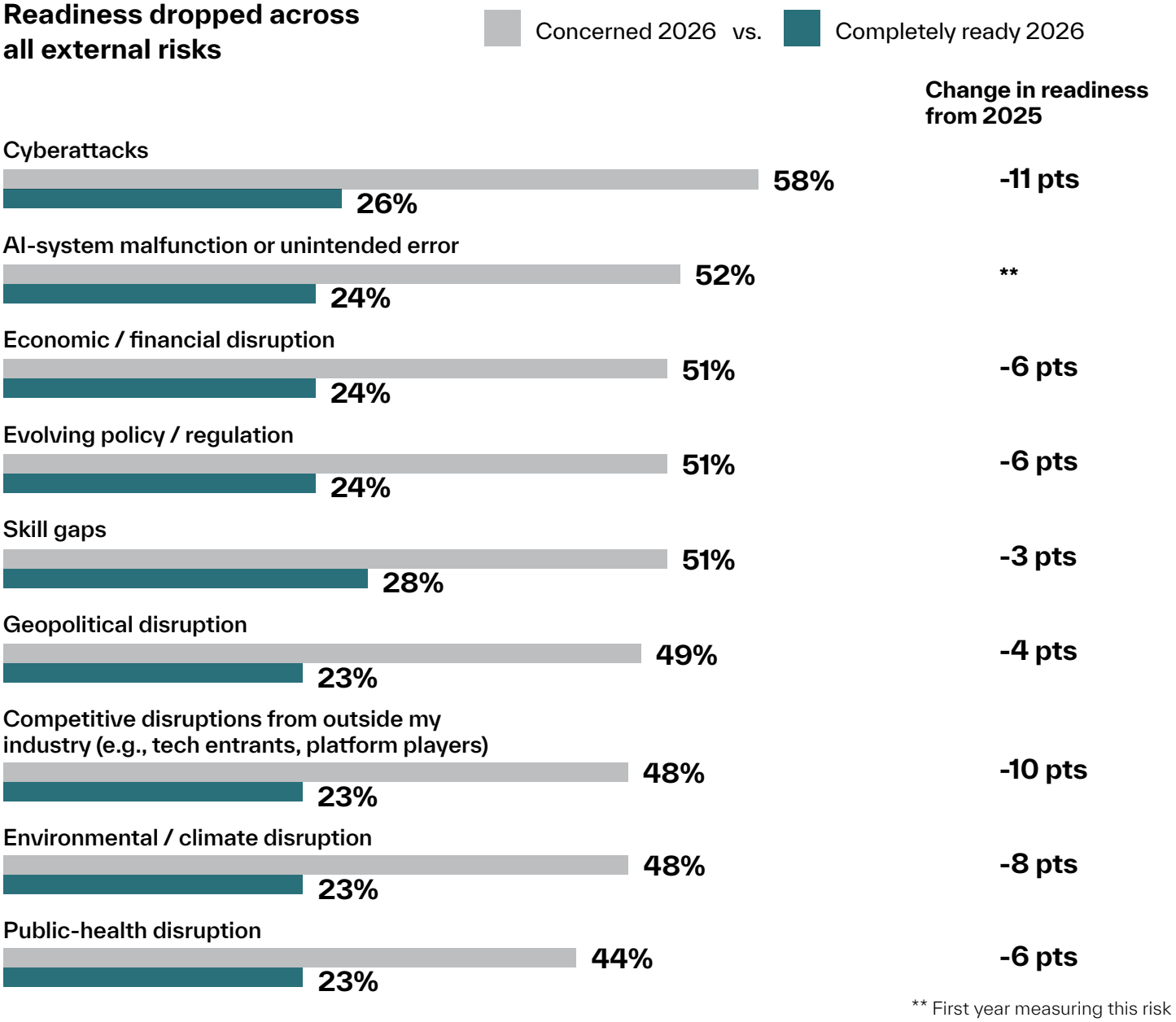
Leaders express a need to update their governance and policies to catch up, yet actions have not yet caught up with intent. In many parts of the world, governments and organizations are taking measures to strengthen digital sovereignty, seeking greater control over their data, technology and critical digital operations amid heightened geopolitical tensions. Control is increasingly being treated as something with economic and strategic value.

The risk environment is becoming more complex

For the third year in a row, concerns about cyber defense top the list of external concerns, as confidence to meet external challenges drops



Readiness dropped across all external risks



** First year measuring this risk

Q15: When thinking holistically about the external risks your organization faces, how concerned are you about each of the following? Q16: How ready would you say your organization currently is to manage the following external business risks? Base: Total (n=3700)

Sovereignty views are running ahead of sovereignty action



65% say sovereignty considerations should shape the entire technology strategy, yet 78% have taken three or fewer of the 10 sovereignty actions and only 6% have taken six or more

Stronger views go with only slightly more action

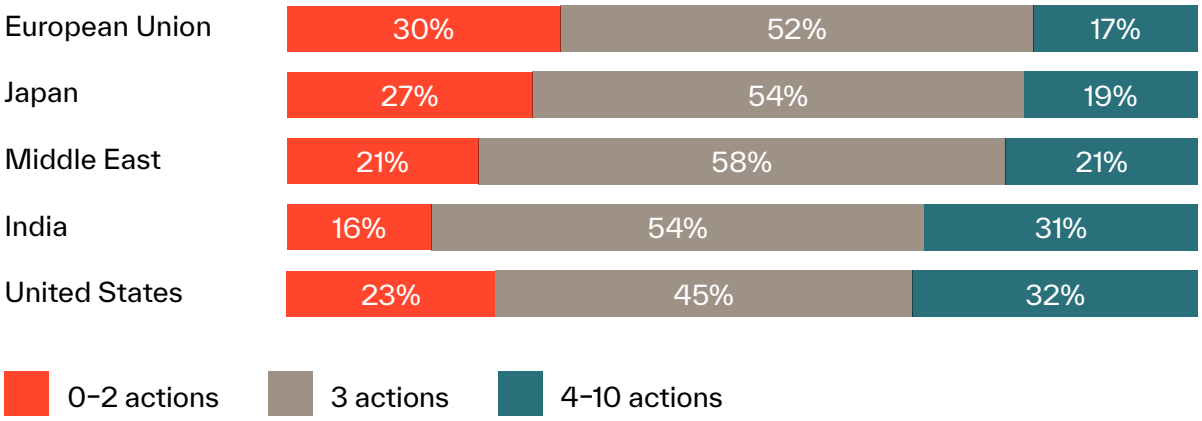
Organizations that say sovereignty should shape the entire strategy have taken 3.2 of the 10 actions on average, compared with 3.1 for those who would limit it to sensitive data and critical workloads, and 77% of leaders have still taken three or fewer

Europe is not more sovereignty-minded than the rest of the world

Across nine European markets, views sit within 3 points of the global figure on all seven trade-offs, and organizations have taken slightly fewer actions (3.0 vs. 3.2 on average)

The EU trails other geographies on digital sovereignty actions

% Selected



Q26: Which of the following actions has your organization taken to strengthen its digital sovereignty? Q27: Which of the following best reflects your organization's perspective on digital sovereignty? Base: Total (n=3700). Numbers may not add up to 100% due to rounding.



Build governance to enable change, not just avoid failure

AI governance should do more than set limits. It should give organizations the clarity to move forward: which uses are appropriate, who owns decisions and how risks will be monitored.

Organizations shouldn't treat governance as a final approval hurdle after an AI solution has been built. Accountability, risk assessment and oversight need to be designed into how the technology will operate. The purpose isn't to eliminate uncertainty before anything moves forward, but to establish how the organization will make decisions and respond when conditions change.

61%

of leaders say AI increases the sophistication of cyber threats

Yet only

28%

say their data governance and management are completely ready to manage future risks and disruptive forces

33%

say they would have implemented stronger governance, risk management and compliance frameworks from the outset of their AI implementations

Stronger governance:

Organizations taking six or more governance actions:

+13 pts more likely to report positive AI/ML returns vs. those taking five or fewer (76% vs. 63%)

+19 pts more likely to be completely ready to implement AI (46% vs. 27%)

+20 pts more likely to be completely ready to manage cyberattacks (45% vs. 25%)

Risk assessments and audits of AI:

Those who report conducting risk assessments and audits, the governance action most strongly linked to positive returns:

+10 pts

more likely to report positive AI/ML returns (70% vs. 60%)

Q16: How ready would you say your organization currently is to manage the following external business risks? Q18: How ready would you say these elements of your organization's IT currently are to manage future risks and disruptive forces? Q20: How much do you agree or disagree with the following statements? Q22: Which of the following actions has your organization taken to strengthen AI governance? Q33: Thinking about the specific digital technologies, tools, or solutions your organization is currently investing in, how would you describe the return on investment (ROI) your company has experienced as a result of these investments? Base: Total (n=3,700), except positive ROI, which is based on respondents investing in AI/ML.

Methodology

The Kyndryl Readiness Report has insights from 3,700 senior leaders and decision makers across 21 countries. The Report uncovers the drivers, barriers and trade-offs that can make or break the ability of organizations to protect, sustain and accelerate their performance and future-proof their mission-critical processes.



21 countries

Australia
Belgium
Brazil
Canada
China
Denmark
France
Germany
India
Ireland
Italy
Japan
Mexico
Netherlands
Saudi Arabia
Singapore
Spain
Sweden
United Arab Emirates
United Kingdom
United States

United States, Japan (n=300); Australia, Brazil, Canada, China, France, Germany, India, Ireland, Italy, Mexico, Spain, United Kingdom (n=200); Belgium, Denmark, Netherlands, Saudi Arabia, Singapore, Sweden, United Arab Emirates (n=100)

24 industries, with a focus on 6 core industries

Banking and financial services
Energy and utilities
Healthcare
Insurance
Manufacturing (including consumer products)
Telecommunications
Others

Banking and financial services (n=664), energy and utilities (n=514), healthcare (n=484), insurance (n=524), manufacturing (including consumer products) (n=555), telecommunications (n=494)

Respondent profiles

Within this report, 50% of respondents are C-Suite level executives, and 50% are senior directors and business unit leaders who influence technology decisions. Half of respondents represented companies with $1 billion or more in revenue. Half represented business leaders (i.e., CEOs, CFOs and their organizations); half represented technology leaders (i.e., CIOs, CTOs and their organizations).

The survey was conducted by Edelman Intelligence on behalf of Kyndryl. Fieldwork was conducted via online survey and telephone interview between July 10 and September 2, 2026.

kyndryl

This report was not printed.

Company Headquarters

One Vanderbilt Avenue, 15th Floor
New York, New York 10017

kyndryl.com

© Copyright Kyndryl, Inc. 2026

Kyndryl is a trademark or registered trademark of Kyndryl, Inc. in the United States and/or other countries. Other product and service names may be trademarks of Kyndryl, Inc. or other companies.

This document is current as of the initial date of publication and may be changed by Kyndryl at any time without notice. Not all offerings are available in every country in which Kyndryl operates. Kyndryl products and services are warranted according to the terms and conditions of the agreements under which they are provided.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Kyndryl has no obligation to develop or release any of the functionality or products described in this statement. Any information about Kyndryl's possible future offerings is subject to change by Kyndryl at any time without notice and does not represent a commitment, promise or obligation for Kyndryl to deliver or make available any offering.