kyndryl

Navigating Cyber Risk & Regulation

A focus on cyber regulation readiness from the Kyndryl Readiness Report

Introduction

The Kyndryl Readiness Report — a global survey of business and technology leaders combined with exclusive data from Kyndryl Bridge, the company's AI-driven digital business platform — sheds light on how business leaders turn to their IT and talent to address business challenges and gain a competitive edge.

As cyber-attackers employ increasingly sophisticated techniques, organizations worldwide are seeing accelerated threats to their mission-critical technology systems. Governments have also taken steps — such as DORA and NIS2 from the European Union, and Japan's legislation on Active Cyber Defense framework — to implement new regulatory measures aimed at protecting citizens and their data from cyber-attacks. The ever-evolving global regulatory landscape remains fragmented: nearly 100 countries around the world are introducing legislation that impacts critical infrastructure.

The pace of these developments have left many organizations unsure of the way forward — 55% say navigating the frequency and speed of policy and regulatory changes is a significant challenge, even as two-thirds say the overall impact of regulation is positive. Cyber regulation readiness is about taking deliberate, proactive measures to safeguard organizations, comply with evolving regulations and swiftly restore systems in the event of an incident.

Small- and medium-sized enterprises, in particular, which typically benefit from agility despite lean staffing and more-limited resources, have faced increased pressure to prioritize their information and communication technology investments. While supervisory regulators acknowledge the proportionality of these risk profiles, this does not mean they lessen their requirements for operational resilience.

In response to new evolving regulations, businesses and organizations across various industries are seeking stronger partnerships to address IT complexity and interconnected systems that could fail during daily operations. And others are considering whether AI can help codify more structured technological resilience into their business frameworks to mitigate risks from third-party failures, software application issues, and other exposures.

Kyndryl leverages its mission-critical expertise to identify gaps in preparedness and recovery pathways — and then implement targeted and relevant solutions. Customers can be paired with Kyndryl experts to identify potential vulnerabilities that threaten their systems' stability and stay ahead of emerging threats.

An Emerging Paradox

The Kyndryl Readiness Report sheds light on a **tech readiness paradox** among business and IT leaders — who express confidence in their current technology posture while expressing concern about its readiness to address future challenges.

WHILE

90%

of leaders are confident their IT infrastructure is best-in-class

ONLY

39%

of those leaders say their IT infrastructure is ready to manage future risks

#1

Leaders say their top concern is cyber-attacks, followed by evolving regulations

Cyber attacks are the #1 concern among business leaders

The “always on” global economy demands reliable, around-the-clock technology: banks, airline ticketing and seating systems, e-commerce sites, healthcare providers, and manufacturers have come to depend on always-available technology to serve them and their customers.

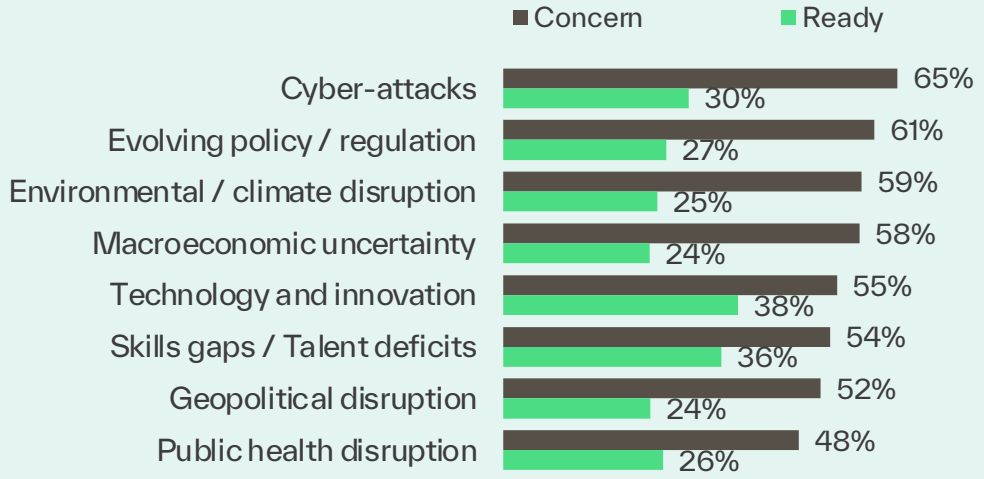
With so much depending on these mission-critical systems, businesses are focused on preventing disruptions and recovering quickly once incidents occur.

Business leaders say their number-one concern is cyber-attacks, followed closely by evolving regulations and environmental disruptions. And while 65% of leaders are concerned about cyber-attacks, only 30% of them say they are completely ready to face them. The gap between concern and readiness will be important to close, but complexity gets in the way.

Leaders also say their technology posture weighs considerably on their overall perception of readiness. Organizations say the #1 way to mitigate their major risks is to upgrade their IT infrastructure, and #2 is to implement robust security measures.

Concern vs. readiness gap

% Concerned vs. % completely ready across external risks



Top risk mitigation actions

% Selected top 3

42%
Upgrading IT infrastructure

38%
Implementing robust cybersecurity measures

31%
Conducting regular risk assessments

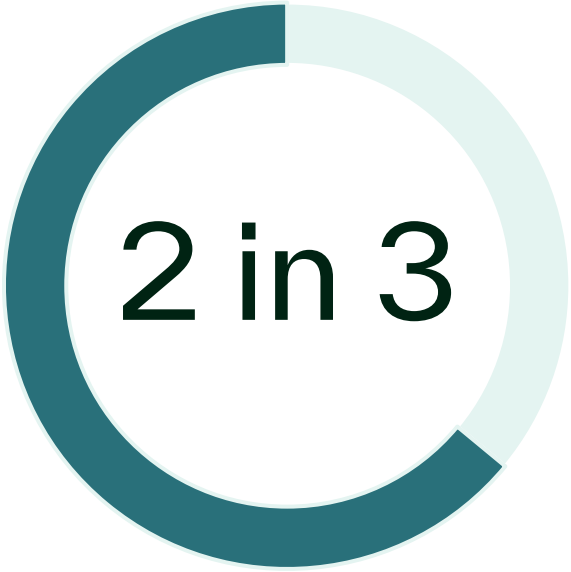
kyndryl

Aging IT estates open the door to increased vulnerability. Better observability can help prioritize tech investments.

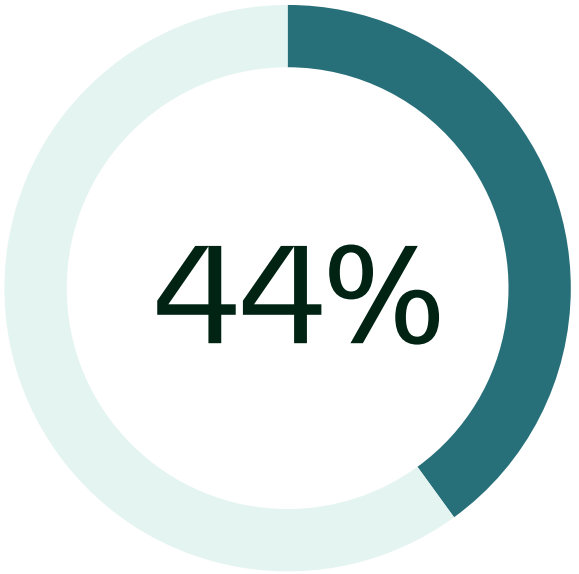
Almost all leaders — 94% — say modernizing their IT is a high priority. They also say updating their IT is the #1 way they are mitigating risks. Yet only 3 in 10 say their organization is leading when it comes to their tech modernization journey. As IT estates continue to age, business leaders say their #1 risk for end-of-life systems is increased vulnerability.

Achieving a balance between security and innovation while keeping pace with emerging threats and monitoring compliance with regulations and standards across complex organizations spanning multiple geographies is further hindered by insufficient visibility of risk across the IT estate.

A new approach is required to help IT, security, and audit work together in new ways to manage enterprise risk. By integrating new and existing tools and technologies from across the enterprise into a unified data platform, IT and security leaders can observe the entire IT estate and continuously monitor key IT controls. When combined with advanced automation and AI, the insights can be used to prioritize tasks, orchestrate teams, technologies and processes, and drive down enterprise risk with improved efficiency.



CEOs are concerned their IT tools or processes are **outdated or close to end-of-life** (64%)



of **servers, storage, networks, and operating systems** are approaching or at end of life, according to Kyndryl Bridge

kyndryl

Business leaders want to modernize, but complexity — in patchwork regulations and in sprawling IT estates — gets in the way

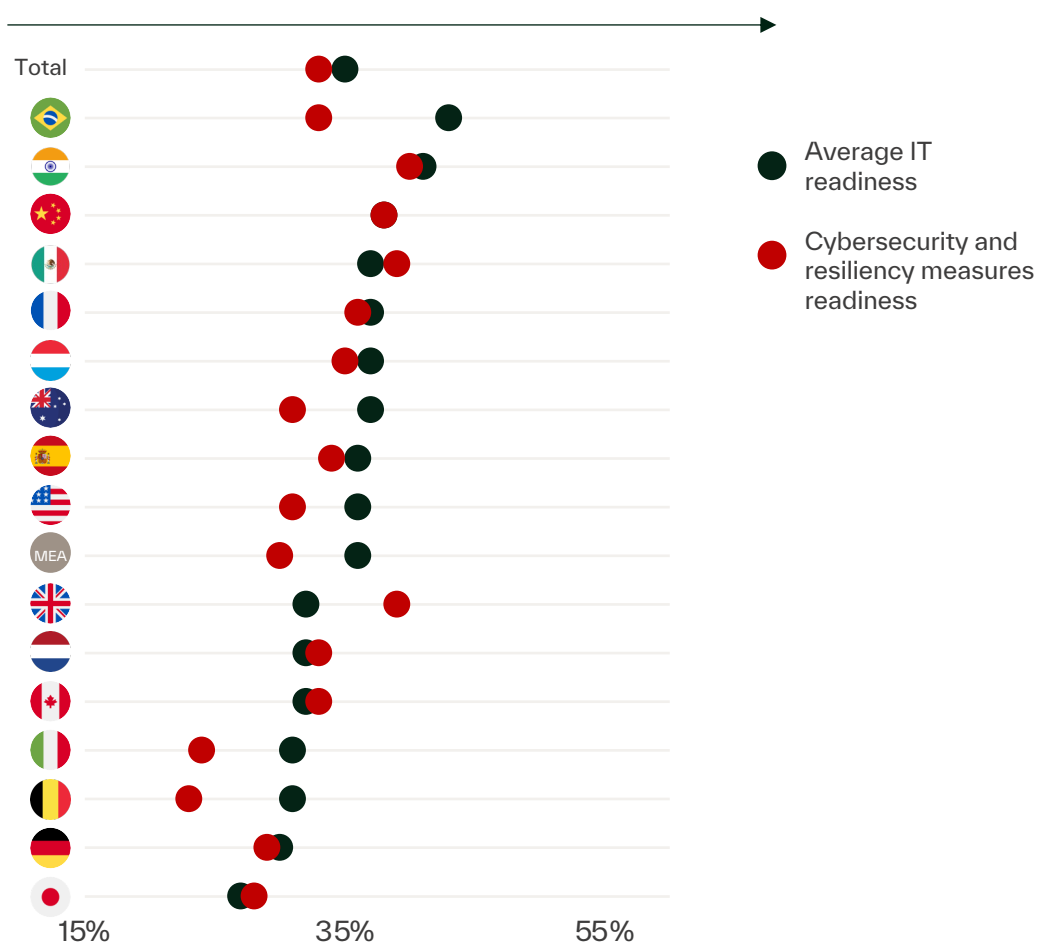
Fast-moving technological advancements and policy decisions have caused C-suite leaders to carefully evaluate steps in technology and innovation that scale to head off future needs. While overall readiness correlates strongly with security and resiliency readiness, other factors, like workforce and regulation readiness, can complicate the picture.

For large enterprises operating globally, one of the main complexities is the fragmentation of regulations. Geography-wide approaches (such as DORA and NIS2 Directive in Europe and Japan's anticipated legislation on Active Cyber Defense framework to strengthen key aims with global standards) are establishing overall shared goals to address evolving challenges and risks associated with the digitization of economies. Regulators are augmenting focus on governance, risk, and disclosure.

Generally speaking, leaders are enhancing overall governance — beginning in the C-suite — for an organization-wide foundation to address 5 main areas of an essential cyber readiness strategy:

1. Threat detection & prevention
2. Automated compliance monitoring
3. Risk assessment & management
4. Data protection & privacy compliance
5. Incident response & remediation

Cyber readiness by market



ONLY

33% of leaders say their security and resiliency measures are completely ready to manage future risks

Modernization projects are often challenged by security and resiliency issues

1 in 4

Report that they have experienced challenges to modernization by relying on **outdated security protocols,** leading to a data breach or cyberattack

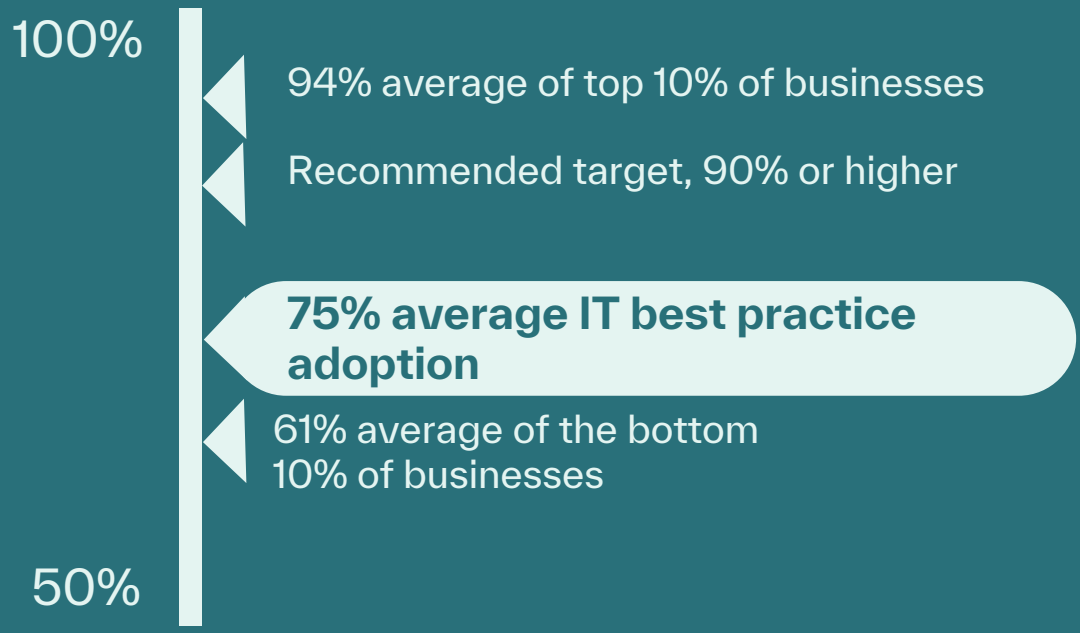
61%

Report that **cybersecurity threats and vulnerabilities are a challenge** in their technology modernization efforts

Kyndryl Bridge empowers organizations to observe their IT estates, allowing them to continuously innovate, achieve higher levels of operational maturity, identify aging software and hardware, and establish a foundation for current and future digital business requirements.

Kyndryl's measure of best practice adoption is a holistic view of effective IT, comprised of industry IT standards and measures for security compliance and regulatory compliance that can be monitored automatically.

% of IT best practice adoption



Source: Kyndryl Bridge data

Ultimately, those leading in tech modernization report higher readiness for external risks, including security risks. Here's what they're doing differently.

Active modernization of IT infrastructure allows leaders to feel more confident and ready in cyber readiness. Businesses further along their tech modernization journey report heightened readiness to navigate overall risks (+11% pts vs. early-stages) and cyber-attacks (+12% pts) and demonstrate four characteristics that set them apart:

1. They prioritize in a way that lets them both run their mission-critical business operations today while transforming for the future
2. They are seeing better ROI on emerging technology (e.g., AI, quantum, edge)
3. They are nurturing talent, skills and culture
4. They are collaborating effectively across the C-suite to achieve business goals

kyndryl

On average, those leading in tech modernization report:

+11% pts

more ready for risks than those in early stages of modernization

+12% pts

more ready for cyber-attacks than those in early stages of modernization

+11% pts

more ready for evolving policies and regulations

kyndryl