



# Building Resilience in a Digital-First World

OCTOBER 2022

Authors:

**Giulia Carosella**

European Digital Transformation Practice Lead

**Anielle Guedes**

Senior Research Analyst, European Customer Insights and Analysis Group

**Ralf Helkenberg**

Research Manager, European Privacy and Data Security

**Francesca Ciarletta**

Research Manager, European Services

IDC #EUR149691722

An IDC InfoBrief, sponsored by

**kyndryl**



# Table of contents



## Navigating this InfoBrief

Click on titles or page numbers to navigate to each section.

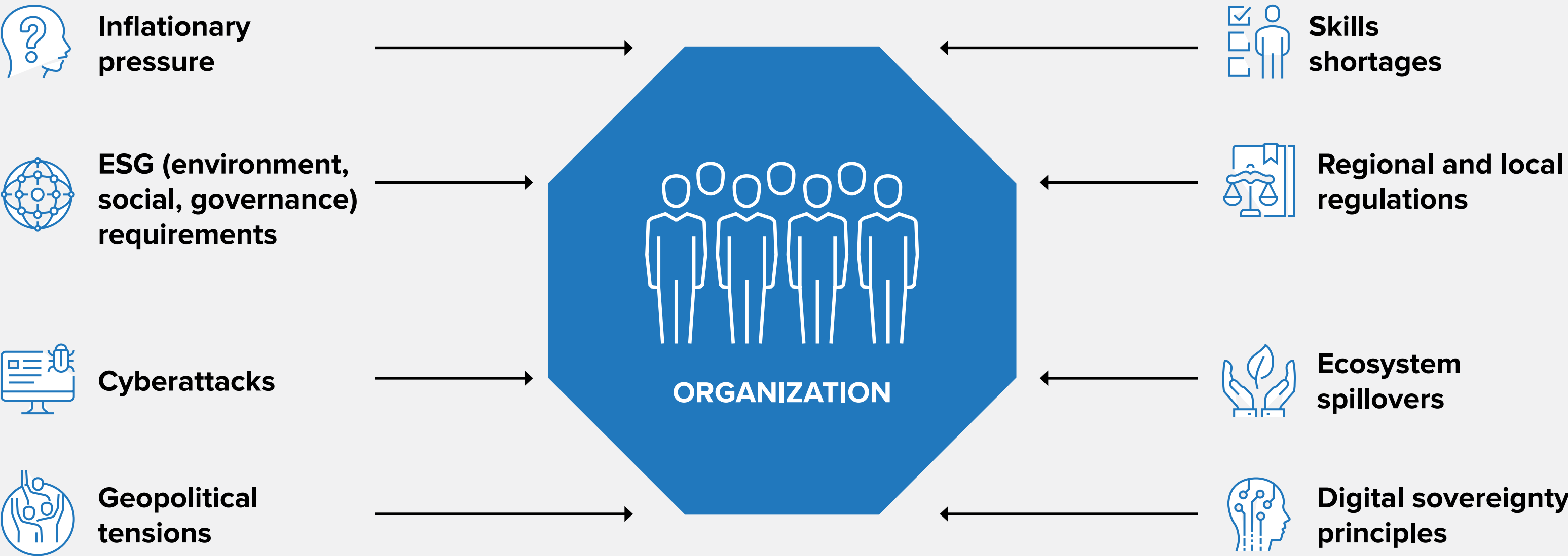
Business leaders face many challenges ...	3
... but organizations are not sufficiently prepared	4
Five operational resilience priorities steering C-suite agendas	5
Resilience imperatives drive evolution of security strategies	6
A fast-moving regulatory landscape pushes companies to comply with new standards	7
Organizations need to enhance ESG strategies to comply with regulations and earn trust	8
Business leaders need to ensure their partner ecosystem is resilient	9
Skill shortages impact operational resilience	10
Lessons learnt from a resilient infrastructure	11

Digital technologies as the foundation of a resilient business	12
A resilient infrastructure is key to delivering business outcomes	13
Invest in IT infrastructure to achieve operational resilience	14
Taxonomy: definition of major threats	15
Message from Kyndryl	16

# Business leaders face many challenges ...

To thrive in a highly dynamic and volatile world, organizations must continuously adapt and innovate. As a result, they increasingly rely on digital capabilities to solve business challenges, manage risks, and deliver on their key priorities. From operational improvement, to reaching new customers and generating new revenue streams, C-suite leaders have learnt that technology is a strategic differentiator to future-proof their organization against threats.

Staying operationally resilient is a key priority for organizations that must grapple with new threats every day, including increasing environmental changes, cyberattacks, and third-party risks — all while new and complex regulations continue to be introduced.



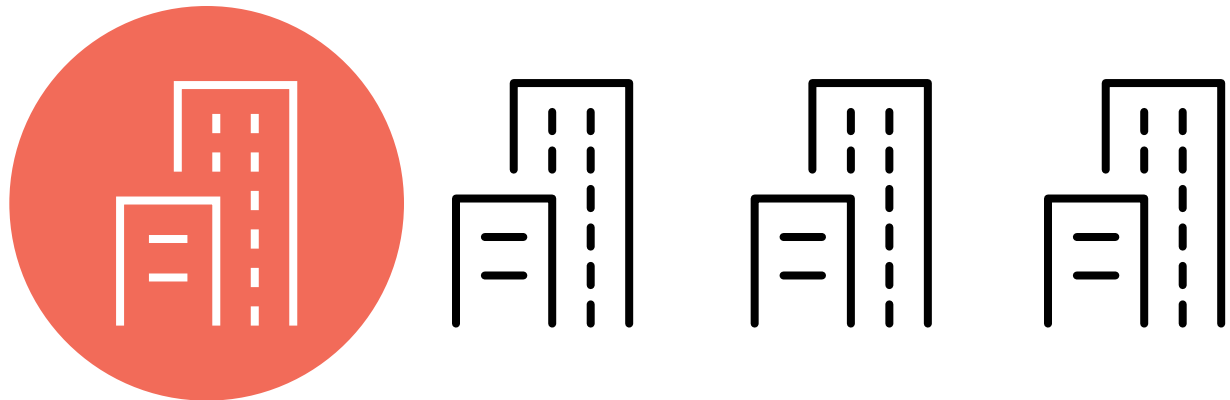
“ By 2023, most C-suite leaders will implement business-critical KPIs tied to data availability, recovery, and stewardship as rising levels of cyberattacks expose the scale of data at risk.

# ... but organizations are not sufficiently prepared



More than **80%** of worldwide organizations think that external threats will have a significant impact on global economic activity.

Only **one in four** organizations is ready to adequately prevent and respond to a disruptive event.



## What is operational resilience?




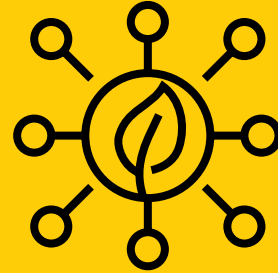

Operational resilience is an organization’s ability to **deliver critical operations** through disruption. With operational resilience, an organization can leverage digital capabilities to:

- **Identify and prevent** threats and potential failures
- **Respond** and adapt to disruptive events
- **Recover** and learn from the impact of disruption on the delivery of critical operations through disruption



# Five operational resilience priorities steering C-suite agendas

C-suite leaders need to focus on five key priorities to respond to continuous market threats and to thrive amid the uncertainty. Those who best address these priorities will be in a stronger position.

	<div>1</div> <div></div>	<div>2</div> <div></div>	<div>3</div> <div></div>	<div>4</div> <div></div>	<div>5</div> <div></div>
	<div>Strengthen <b>cyber resilience</b></div>	<div>Deepen due diligence on regulatory <b>compliance</b></div>	<div>Sharpen <b>ESG</b> strategies</div>	<div>Manage <b>ecosystem</b> <b>risk</b> spillovers</div>	<div>Bridge the <b>skills gaps</b></div>
Responsible C-suite personas	<ul style="list-style-type: none"><li>CIO, CTO, CDO</li><li>CRO, CISO</li></ul>	<ul style="list-style-type: none"><li>CEO</li><li>CIO, CTO, CDO</li><li>COO</li><li>CRO, CISO</li></ul>	<ul style="list-style-type: none"><li>CEO</li><li>CMO</li><li>CHRO</li><li>CSO (sustainability)</li></ul>	<ul style="list-style-type: none"><li>CEO</li><li>CIO, CTO, CDO</li><li>COO</li><li>CPO</li><li>CMO</li></ul>	<ul style="list-style-type: none"><li>CEO</li><li>CIO, CTO, CDO</li><li>CHRO</li><li>CPO</li></ul>

# Resilience imperatives drive evolution of security strategies

KEY C-SUITE PRIORITY:  
Strengthen **cyber resilience**



## The growing cyberthreat landscape



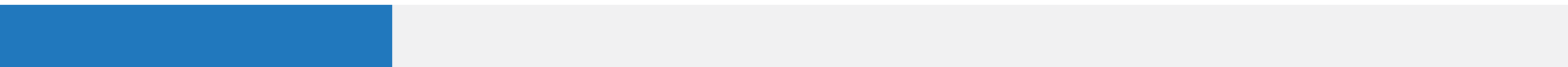
Cyberattacks are growing in volume, variety, complexity, and precision:

**54%** of organizations have experienced an increase in the volume of cyberattacks in the past 12 months.



Ransomware is the biggest cyberthreat for organizations:

**25%** of ransomware victims experienced business disruption of a week or more.



## Cyber resilience — a strategic imperative



(IDC Worldwide CEO Survey, January 2022)

CEOs recognize that security must keep pace with the evolving cyberthreat landscape.

The growing cost and disruptive nature of cybersecurity incidents requires organizations to strengthen their cyber resilience to ensure operational and business continuity with minimal impact.

# A fast-moving regulatory landscape pushes companies to comply with new standards

KEY C-SUITE PRIORITY:  
Deepen due diligence on  
regulatory **compliance**



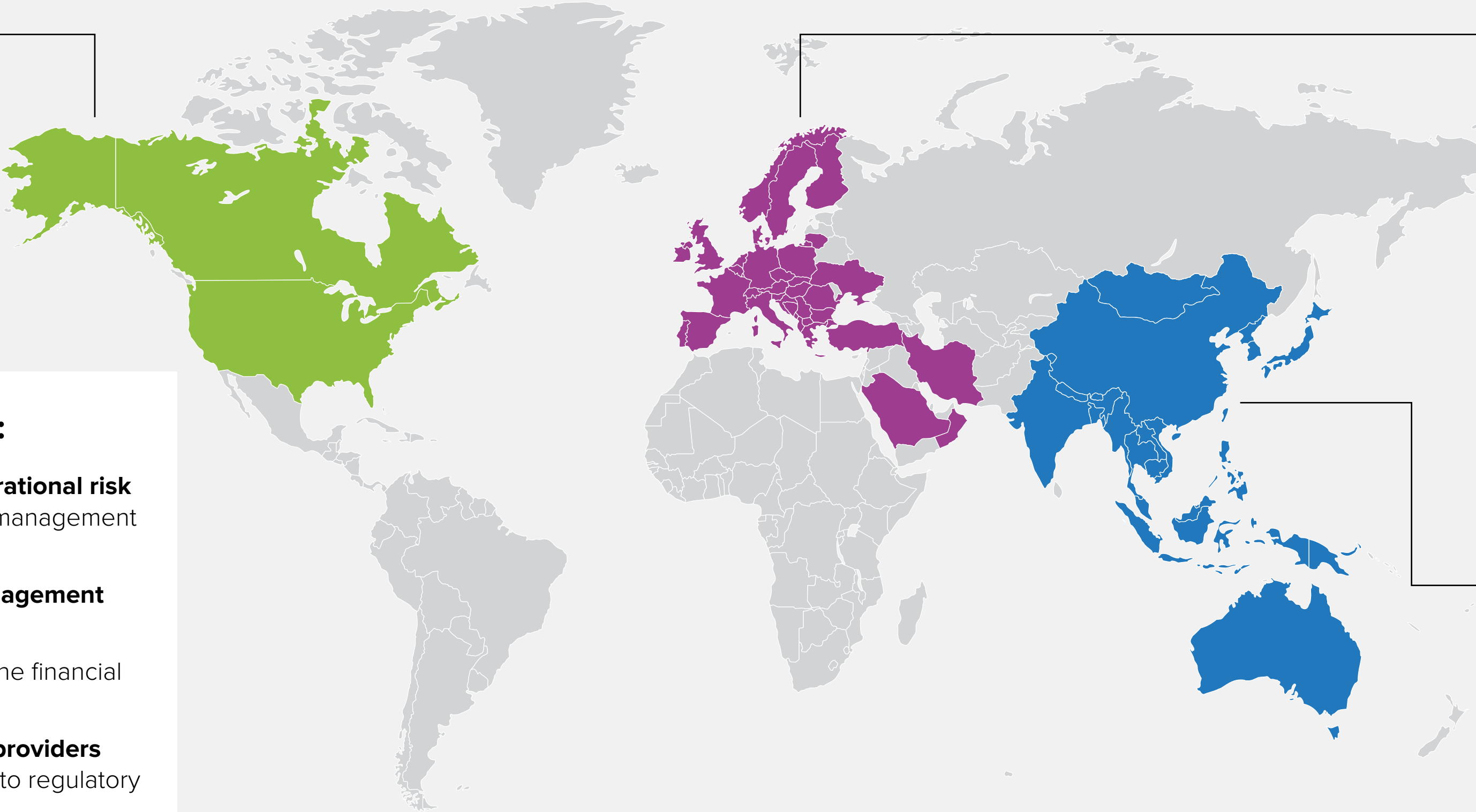
## Key current and upcoming legislation related to operational resilience\*:

### North America

- USA Part 29 — Protected Critical Infrastructure Information
- Canada Emergency Management Act
- Canada Treasury Board Secretariat’s (TBS) Policy on Government Security
- Federal Financial Institutions Examination Council (FFIEC)

### Emerging themes across geos:

- Continued focus on strengthening **operational risk management** with an eye on controls management and **regular mandatory testing**
- Standardization of **third-party risk management** frameworks, processes, and standards
- Laser focus on **concentration risks** in the financial sector
- Recognition of **critical ICT third-party providers (CTPs)** and enforcing their compliance to regulatory standards by direct regulation



### EMEA

- EU Digital Operational Resilience Act (DORA) (financial services)
- EU Network and Information Security 2 Directive (NIS2)
- UK’s Operational Resilience Framework (financial services)
- UAE, Kuwait, Qatar, Bahrain, National Cybersecurity Strategy
- Central Bank of UAE, Banking Control Regulation in KSA — SAMA, South African Reserve Bank (SARB), specific resilience and BCM principles

### Asia/Pacific

- India CERT-In Cybersecurity Directions 2022
- China’s Data Security Law
- Australia Security of Critical Infrastructure Act 2018

# Organizations need to enhance ESG strategies to comply with regulations and earn trust

KEY C-SUITE PRIORITY:  
Sharpen **ESG** strategies



Climate change, rising energy prices, and evolving regulations (e.g., the European Corporate Sustainability Reporting Directive) are pushing organizations to rapidly implement elements of corporate and social responsibility in their business strategies.



**CEOs, CIOs, and chief sustainability officers are focusing on reprioritizing technology investments** with a focus on environmental sustainability, such as cloud service procurement (greener datacenters).



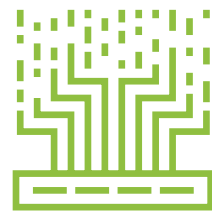
**CMOs, CHROs, and chief sustainability officers are focusing on developing clear** messaging about sustainable technology initiatives (e.g., improved ranking in a sustainability index) to strengthen brand trust.

82%

of CEOs think digital technology investments will significantly drive their ability to meet ESG goals.



## Technology can play a dual role with respect to ESG objectives:



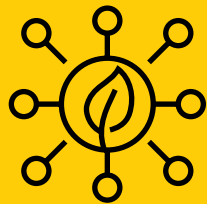
Making technology itself more sustainable, such as reducing datacenter energy consumption.



Helping to meet ESG goals, such as better use of data and analytics to reduce CO<sup>2</sup> emissions, software to track ESG-related KPIs to report and measure the impact, and tech for society and inclusion (e.g., AI-based human rights tracking).






# Business leaders need to ensure their partner ecosystem is resilient

KEY C-SUITE PRIORITY:  
Manage **ecosystem** spillovers



Enterprises need full visibility of their IT supply chain dependencies and the risks and potential business impact associated with third-party providers should one or multiple suppliers fail to provide IT services deemed critical to the business while assessing the suppliers’ operational resilience.

## Risks associated with ecosystem interdependency include:

-  **Provider dependency**
-  **Loss of control**
-  **Less negotiation power**
-  **Greater IT complexity**
-  **Increased regulatory and compliance risks**

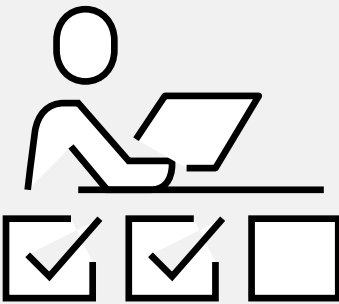
## Enterprises increasingly rely on third-party providers for datacenters and cloud

IT infrastructure spending by 2024



# Skill shortages impact operational resilience

KEY C-SUITE PRIORITY:  
Bridge the **skills gaps**



On average, skill shortages lead to a **4-month** delay in completing digital projects.

Demand is greatest for IT security and IT operations professionals.



**39%**  
IT security professionals



**33%**  
IT operations professionals

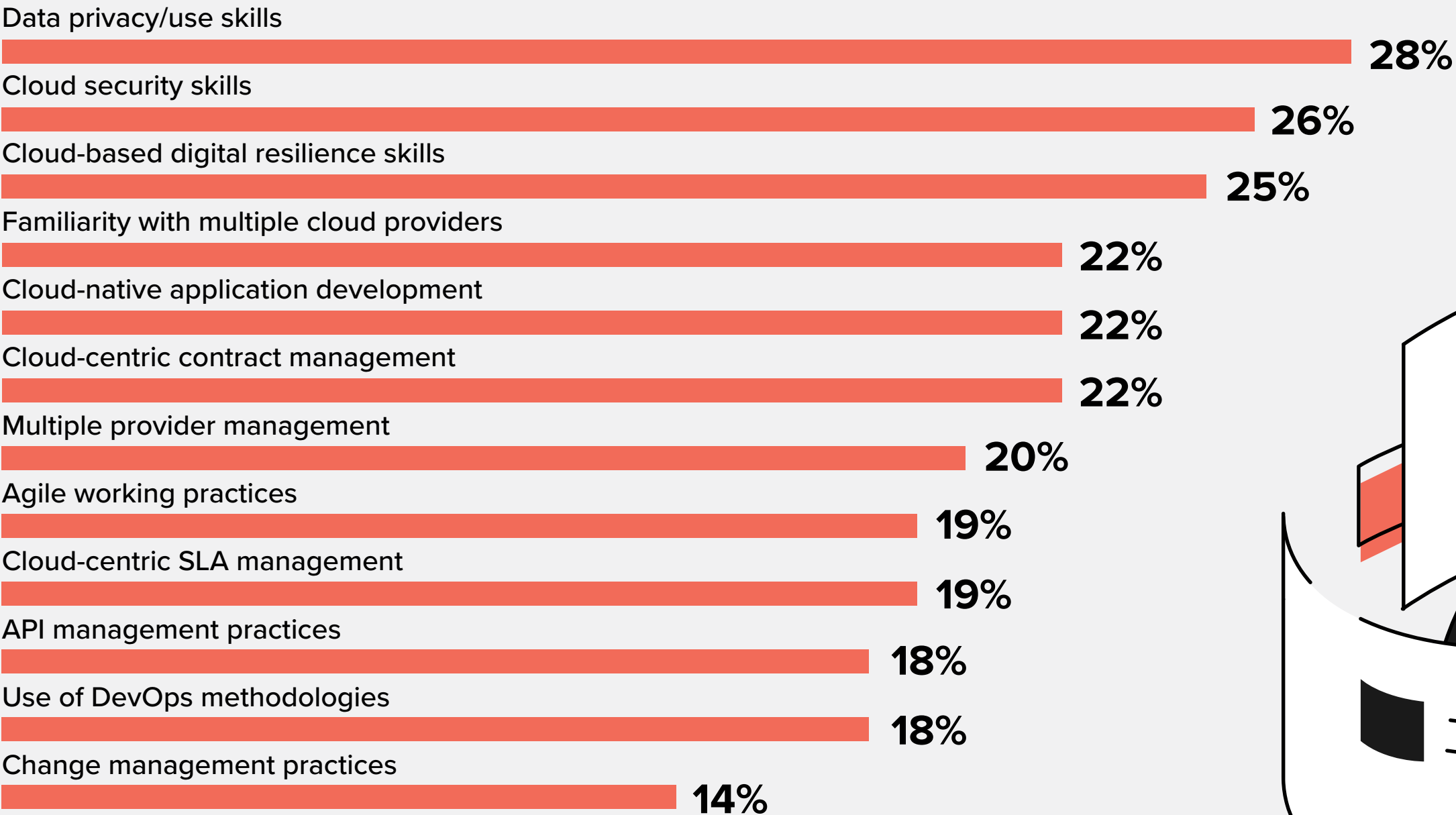


**31%**  
IT project managers

Q. Which technology roles are most in demand for key tech initiatives?

Most organizations around the world say it is difficult to recruit people with data privacy and security skills. Some organizations can acquire or develop these skills in-house. Others will seek help from service providers to fill the gaps.

## Top operational skills needed worldwide



Q. What are the operational skills your organization will most need to develop its own IT and development teams in the next two years to take full advantage of your cloud platform approach?



# Lessons learnt from a resilient infrastructure

For companies to thrive amid the uncertainty and to be successful in the digital economy, it's crucial to incorporate the lessons learnt from previous disruptive events to improve resilience.

## Key lessons learnt



### Likelihood of crisis:

We live in a global, interconnected world in which new threats are more likely than ever.



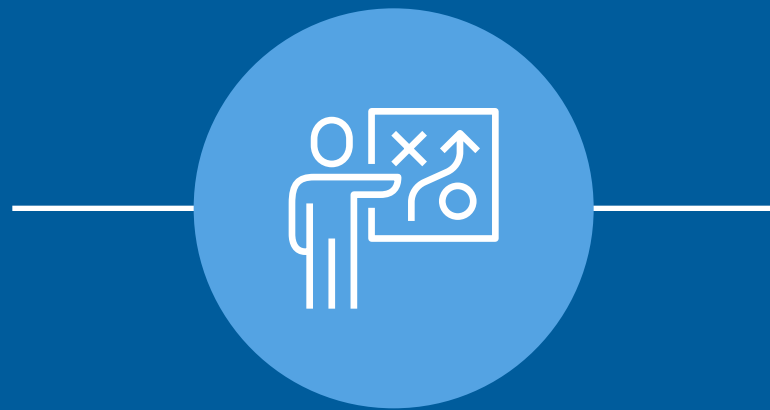
### Continuous change:

Resilience isn't a one-time transformation. It requires the continuous alignment of people, processes, and technology.



### Business criticality:

IT infrastructure resilience determines an organization's abilities to deliver on its business mission and priorities.



### Leadership alignment:

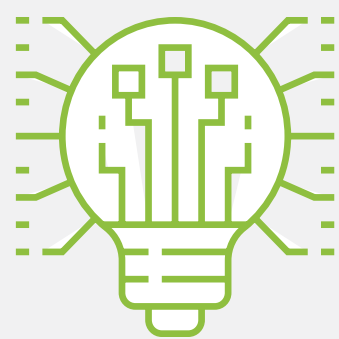
Having tech leads and business leads think about IT and business resilience separately limits companies' ability to respond to new disruptions.

## The value of resilient IT infrastructure

Business processes and value chains are underpinned by technology. This demands close cooperation between IT and business operations.

# Digital technologies as the foundation of a resilient business

## Digital transformation investments boost business resilience



**42%** of organizations globally experienced an annual business resilience improvement of **25% and above** as a result of digital investments.



*Q. Business resilience — What annual percentage improvement in 2021 did your organization experience in each of the following as a result of investments in digital transformation?*

## Organizations believe that they can improve resilience by investing in public cloud, security, and hybrid work:



Source: IDC EMEA Managed CloudView Survey, July 2021 (n = 400)

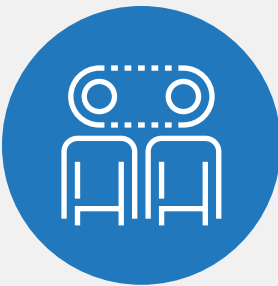
# A resilient infrastructure is key to delivering business outcomes

Most businesses look at resilience as a cost to the business, but resilience drives value as it deals with what is unknown, changeable, unpredictable, and improbable — and has significant consequences. Resilient businesses can quickly adapt to ever-changing market conditions and survive and thrive in a challenging economic, environmental, security, ecosystem, and regulatory landscape. As a result, they can achieve better results across key metrics, from greater profit improvement to quicker time to market.

## Key business outcomes from operational resilience



## Key resilience metrics to keep an eye on



### Brand sentiment and sustainability

E.g., customer sentiment, number of security incidents, ESG performance



### Business risk reduction and regulatory compliance

E.g., key risk indicators (KRIs), violations of laws and regulations, mean time to issue discovery



### Data-driven decision making

E.g., time to recovery, order and delivery lead time



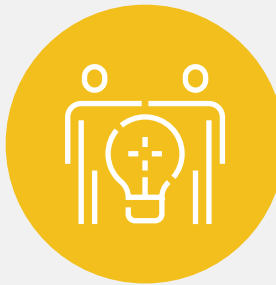
### Employee productivity and retention

E.g., employee advocacy rate, number of agile teams



### Customer experience and digital engagement

E.g., diversity of partnerships, customer response time, mean time to issue resolution



### Business agility and innovation

E.g., innovation rate, crisis response and recovery time

# Invest in IT infrastructure to achieve operational resilience

C-suites have an opportunity to demonstrate their agility, to weather the emerging threats and lay the foundations for future success by adopting **operational resilience by design** into their operating model. Those who are prepared will be able to gain competitive advantage; those who are not could find themselves falling behind and more exposed to future disruption.

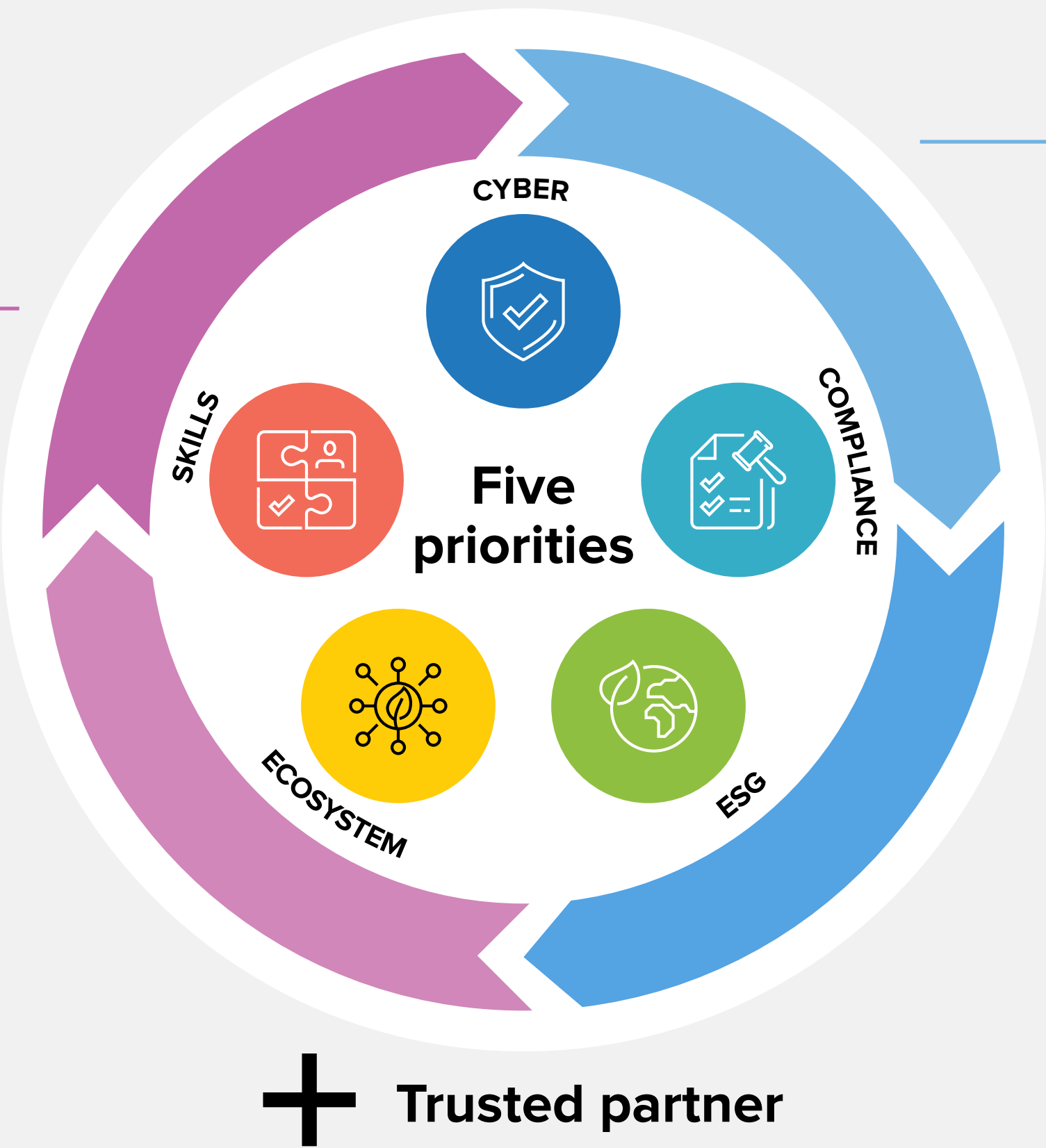
## The “virtuous cycle” to address the five operational resilience priorities:

### Monitor and sustain

- ✓ Develop proper **resilience-related KPIs** across the five priorities

### Implement and test

- ✓ Implement methodologies, **tools, and procedures to prevent, respond, and restore operations**



### Assess and evaluate

- ✓ Understand **your risk universe**
- ✓ Assess **your resilience readiness**
- ✓ Consider **interdependencies across the different parts of the organization**; a data breach, for example, can threaten customer relationships, brand trust and reputation, and finally, financials

### Plan and design

- ✓ Adopt **operational resilience** by design
- ✓ Design tools and plans and identify key roles to prevent and overcome storms of disruption
- ✓ Comply with **regulations and industry standards**

# Taxonomy: definition of major threats



**Geopolitical tensions:** volatility linked with geopolitical events such as the Russia-Ukraine War — a critical geopolitical turning point for Europe and the world



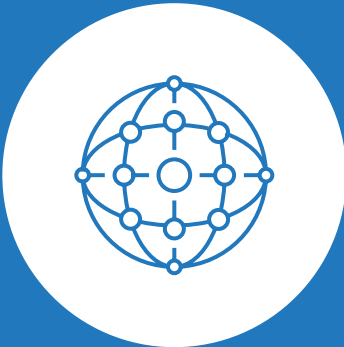
**Skill shortage:** organizations struggling to find qualified workforce with digital capabilities (i.e., lack of qualified workforce for digital technologies)



**Cyberattacks:** increase in cybersecurity threats, also fostered by recent geopolitical events and larger attack surfaces as organizations become more digital



**Inflationary pressure:** high price level increase related to higher cost of energy and lack of tech components, minerals, and materials



**ESG (Environmental, Social and Governance) requirements:** new sustainability initiatives as well as national and supranational regulations are pushing businesses toward a more sustainable approach to ESG



**Digital sovereignty principles:** governments and companies are strengthening their control over their data, hardware, and software to improve resilience against future challenges



**Ecosystem spillovers:** disruption linked with ecosystem partners, including supply chain disruptions and exposure to partners' and customers' vulnerabilities



**Regional and local regulations:** changes in the regulatory environment or in the policy strategy of the geographies in which an organization operates, causing short-term and long-term impact on the business, technology, or market strategy of an organization or industry

# Message from Kyndryl

The accelerated push to digitization has introduced new priorities for the C-suite, such as cyber resilience, regulatory compliance, ESG strategies, ecosystem spillovers, and skills shortages.

Organizations need to be prepared in terms of operational resilience to ensure they can deliver critical business services through any disruptions.

Kyndryl Cyber Resilience provides the expertise, services and technologies that help enterprises anticipate, protect against, withstand, and recover from adverse conditions, stresses, attacks, and compromises of cyber-enabled services.

**Kyndryl works at the core of businesses that move the world. With more than 90,000 skilled professionals serving customers in over 60 countries, we design, build, manage, and modernize the mission-critical technology systems that the world depends on every day.**



For more information, please visit <https://kyndryl.biz/cyberresilience>

kyndryl™

# About IDC



International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

## IDC UK

5th Floor, Ealing Cross,  
85 Uxbridge Road  
London  
W5 5TH, United Kingdom  
44.208.987.7100  
Twitter: @IDC  
idc-community.com  
www.idc.com

## Corporate Headquarters

140 Kendrick Street,  
Building B, Needham,  
MA 02494 USA  
508.872.8200  
www.idc.com

## Copyright Notice

---

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or [permissions@idc.com](mailto:permissions@idc.com). Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit [www.idc.com](http://www.idc.com). For more information on IDC Custom Solutions, visit [http://www.idc.com/prodserv/custom\\_solutions/index.jsp](http://www.idc.com/prodserv/custom_solutions/index.jsp).

Corporate Headquarters: 140 Kendrick Street, Building B, Needham, MA 02494 USA P. 508.872.8200 [www.idc.com](http://www.idc.com)

© 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.