Building organisational resilience: be ready, be prepared, be resilient

Foreword

We're excited to share this publication on building organisational resilience, offering practical insights into how you can boost preparedness, enhance responsiveness, and build long-term adaptability in a world of constant change. This perspective draws from recent global and regional observations, including insights from the Business Resilience Insight Survey and PwC 29th Global CEO Survey 2026, highlighting the evolving and interconnected risk landscape shaping today's business priorities.

Across industries, organisations face a wide range of disruptions, from geopolitical tensions, climate risks, and regulatory changes to cyber incidents, operational failures, and workforce challenges.These disruptions test agility and reveal broader implications for governance, stakeholder trust, and strategic outcomes. The growing pressures from competition, cyber threats, operational disruption failure, and regulatory complexity highlight the need to embed resilience throughout the organisation.

Our experience shows that resilience capabilities frequently develop in silos, with gaps remaining in areas such as scenario coverage, testing frequency, technical dependency mapping, and crisis response coordination. In many cases, plans exist but are not regularly updated or tested against realistic disruption scenarios, limiting their effectiveness when disruptions occur.

Building resilience requires more than response plans, it calls for developing the right mindsets, modernising operating models, and empowering leaders to manage uncertainty with clarity and confidence. This includes strengthening governance and alignment across business and technology functions, embedding regular review and exercise cycles, and investing in people and enabling technologies. Continued investment in resilience culture, technology, and leadership development is crucial for anticipating future risks and maintaining operational continuity. Digital transformation, including emerging technologies and generative AI, further underscores the importance of equipping your workforce with the skills and tools to adapt swiftly.

We believe a robust resilience programme by aligning business objectives, ICT capabilities, third-party dependencies, and workforce readiness is key to ensuring stability and long-term value creation. By embedding resilience into daily operations, strengthening governance, and continuously testing preparedness, organisations can better respond to disruption, protect stakeholders, and maintain trust in an evolving risk landscape.

We hope this publication offers useful insights and guidance to support your resilience journey. By understanding current challenges and emerging priorities, you can build stronger foundations to navigate uncertainty and seize future opportunities.

Sincerely,

Yuliana Sudjonno
Partner
PwC Indonesia

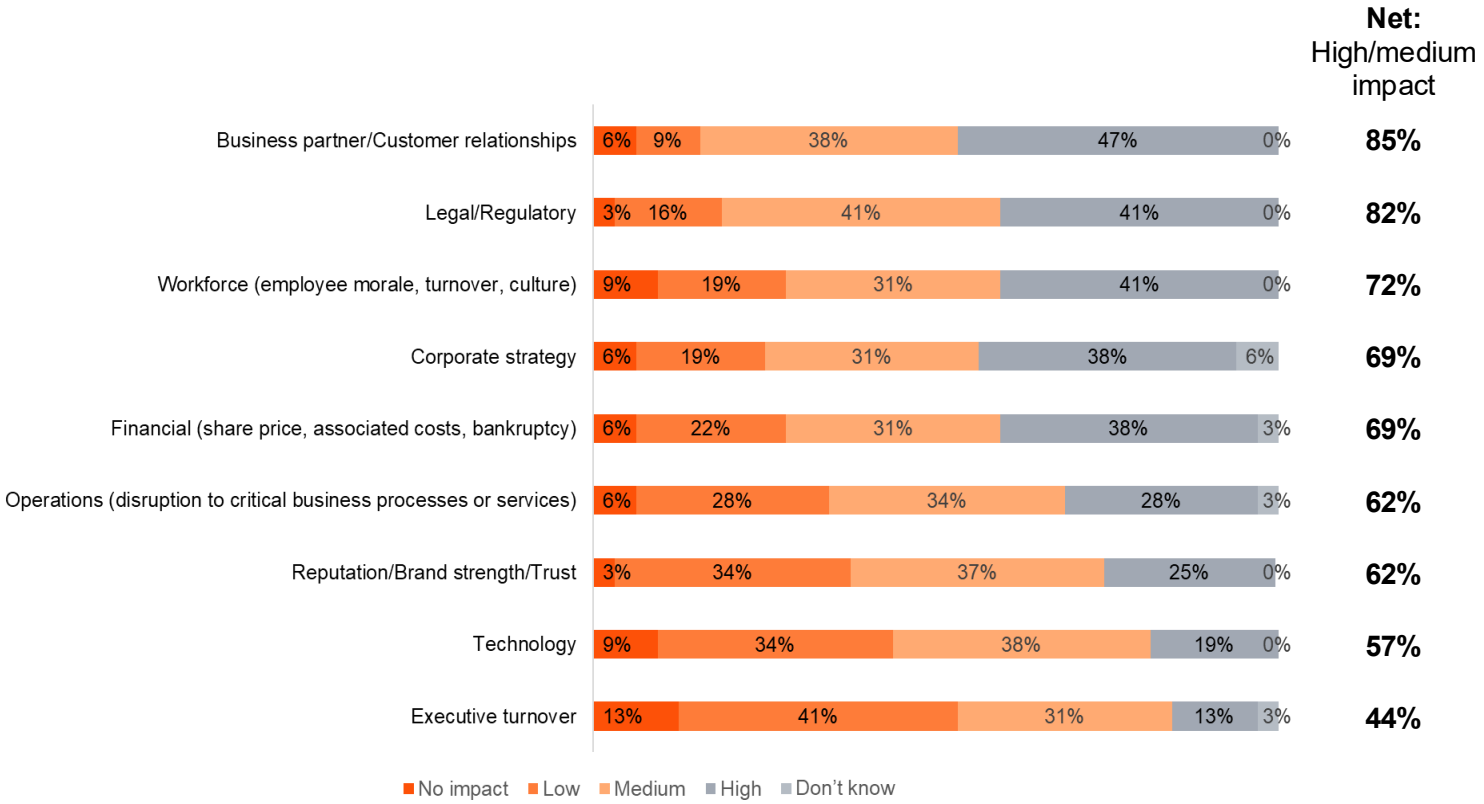
Navigating disruption trends and organisational risks

In today's fast-paced world, organisations face a myriad of challenges that threaten their stability and long-term success. Recent insights show that 63% **of companies have** encountered major disruptions in the last two years. Geopolitical tensions and climate risks are among the top disruptions.

Excluding pandemics, geopolitical tensions, and climate risks, the most disruptive risks to organisations include:

1. Legal/regulatory
2. Competitive/marketplace disruption
3. Cyberattacks
4. Operational disruption or failure

The impact of these risks is profound. Organisations report strained relationships with business partners and customers, increased legal and regulatory exposure, and workforce issues. These challenges highlight the extensive effects disruptions can have across an organisation.



Looking ahead, businesses are increasingly wary of future disruptions. Key risks include rising competitive pressures, ongoing cyber threats, complex regulatory changes, employee retention and recruitment challenges, and geopolitical disruptions. The PwC 29th Global CEO Survey 2026 echoes this, identifying competition, cyber risk, and regulatory environments as major strategic. Cyber risk now stands alongside macroeconomic volatility as a top concern for chief executive officers (CEOs), with both seen as potential sources of significant financial loss.

Geopolitical instability is also contributing to rising climate-related pressures by affecting energy resources, supply–demand stability, and environmental commitments, which ultimately increases uncertainty and places additional demands on organisational resilience. The link between past and anticipated disruptions underscores the critical need for resilience. Organisations must develop proactive, adaptable capabilities aligned with evolving business priorities to navigate current and future challenges effectively.

Drawing from both the disruptions highlighted above and our practical experience supporting clients through complex events, a number of common challenges tend to surface during disruptions. In practice, leaders are often forced to respond with incomplete information, make trade-offs under tight timeframes, and coordinate across functions and third parties while core systems and resources are constrained. These dynamics can slow situational assessment, complicate response prioritisation, and create disconnects in communication and accountability. These challenges frequently shape how well an organisation can respond and recover.

Challenges during disruptions

Organisations face common challenges during disruptions, such as:

- Limited access to sufficient and timely information
- Difficulty prioritising responses to disruptions
- Ineffective internal and external communication

Assessing preparedness and readiness

Organisations anticipate continued uncertainty, which is evident in the differing levels of preparedness within resilience programmes. The strengthening of these programmes is largely influenced by new risks, regulatory demands, market and industry expectations. Most indicate improved readiness and more cohesive practices in:

Business continuity planning (BCP)[1] - documented information that guides an organisation to respond to a disruption and resume, recover, and restore the delivery of products and services consistent with its business continuity objectives

Disaster recovery plan (DRP)[2] - clearly defined and documented plan which recovers information and communication technology (ICT) capabilities when a disruption occurs

Governance model - mechanism applied by the Board and management to translate elements of the governance framework into the corporate governance infrastructure, including, among others, defined call trees for escalation when disruptions occur and urgent decisions are required.

Footnote:
1. ISO 22301 (2019)
2. ISO 27031 (2016)

However, areas like enterprise crisis plans, cyber recovery and scenario-specific playbook, and the regular updating of testing scenarios also need further development. Many organisations still rely on outdated or limited scenarios that do not fully reflect the range of disruptions that could realistically impact their operations. This uneven readiness shows that while some resilience components are strong, others need significant investment and development.

Organisations are navigating both structural and operational challenges that hinder the development of robust resilience programmes. Structurally, limited understanding at the top, the absence of a clearly defined framework, and unclear direction often cascades through the organisation, leaving working-level teams without the guidance needed to act consistently. Operationally, challenges emerge during execution. For example, when vendors are unable to meet required service levels or recovery timelines, creating gaps between plans and real-world capability. Many are grappling with limited team capacity, as designated resources are scarce. The lack of personnel with the appropriate resilience of knowledge and practical experience is another significant challenge. But what's standing in the way of aligning resilience efforts with a clear operating model? This misalignment often leads to fragmented implementation and inconsistency across functions. Furthermore, maintaining a resilience programme isn't just about keeping up – it's about evolving with organisational growth, adapting to changing operating contexts, and anticipating new threats. Now's the time to rethink how you work and invest in continuous improvement.

Preparing an effective resilience programme

A resilience programme is key to organisational strength, extending beyond response plans to align with business objectives and ICT capabilities. Challenges arise when programmes operate in silos, leading to confusion during crisis response. Misalignment between ICT recovery timelines and business workarounds can further hinder readiness.

Assessing the effectiveness of your resilience programme

Despite the availability of resilience programmes (such as business continuity plans, crisis management plans, disaster recovery plans, etc.), organisations need to periodically review them to ensure alignment between risks, resilience initiatives, business goals, and stakeholders' expectations. Effective resilience requires adaptability and regular updates to keep pace with emerging risks and technologies.

Resilience programmes lose effectiveness when they are isolated or not regularly updated. To support stability and preparedness, resilience initiatives must be integrated into current strategies and maintained as adaptive.

Include the resilience programme updates on the Board agenda to ensure the involvement of the Board and to gather timely feedback for the resilience programme.

Conducting regular exercise and simulation

Simply having a documented programme is insufficient; organisations should develop team muscle memory through regular exercises.

The goal of these exercises is to assess the adequacy and relevance of the current resilience programme, as well as to enhance understanding of roles and responsibilities during crisis response and recovery. Therefore, organisations should conduct exercises and simulations using scenarios relevant to their context while taking into account their level of maturity.

Building resilience awareness

Embedding resilience into daily culture means ensuring all employees understand its significance for business continuity and personal well-being. This is achieved through regular training, onboarding with resilience themes, and internal awareness campaigns. Transparent communication and ongoing education help alleviate employee overwhelm, building trust and readiness for uncertainty.

Upskilling future leaders

Developing future leaders is vital for a resilient organisation. Leaders must guide teams through uncertainty with clarity, empathy, and assurance. Structured programmes should focus on adaptive leadership, crisis decision-making, strategic communication, and change management. Trust and cultural support are essential motivators, especially during rapid transformation. Equipping leaders with these skills enables effective communication of change, builds confidence, and fosters a resilient culture.

Leveraging technology enablement

Technology drives organisational resilience by supporting rapid anticipation, response, and recovery from disruptions. Investment in digital tools for crisis communication, real-time information sharing, and scenario planning is essential. Training employees on emerging technologies, especially generative artificial inteligence (AI), boosting confidence and capability in a tech-driven world. Integrating technology into resilience strategies and upskilling employees enhances operational readiness and future workforce motivation.

Resilience as a strategic imperative

Resilience is crucial not only for current operations but also as a foundational element of long-term business strategy. Implementing a comprehensive resilience programme ensures preparedness, protects stakeholders, and secures ongoing business continuity in an evolving risk landscape.

Strategic focus areas for resilience

Amidst uncertainty, organisations recognise the need for thorough preparation to maintain business continuity. As they look to the future, companies are prioritising:

1. **Resilience programme:** While organisations may have established resilience programmes, the continuously changing risks and uncertainties drive them to regularly update and adapt these programmes to ensure they remain relevant and effective for their specific needs.
2. **Resilient culture and awareness:** Over half of respondents see this as crucial area for the future, emphasising that resilience is rooted in people and a shared mindset.
3. **Technology enablement:** Nearly half prioritise technology, recognising the need for advanced tools and digital capabilities to anticipate risks and maintain continuity.
4. **Upskilling future leaders:** About one-third highlight leadership development for crisis decision-making and coordination.
5. **Resilience metrics and competencies:** While important, these areas are often seen as longer-term goals.

Your PwC Indonesia contacts

Yuliana Sudjonno
Partner
yuliana.sudjonno@pwc.com

Subianto
Partner
subianto.subianto@pwc.com

Andrew Tirtadjaja
Director
andrew.tirtadjaja@pwc.com

Gleny
Senior Manager
gleny.gleny@pwc.com

PwC Indonesia

Jakarta
WTC 3
Jl. Jend. Sudirman Kav. 29-31
34th, 36th-43rd Floor
Jakarta 12920 – Indonesia
T: +62 21 5099 2901 / 3119 2901
F: +62 21 5290 5555 / 5290 5050

Surabaya
Pakuwon Tower
Tunjungan Plaza 6, 50th Floor,
Unit 02-06
Jl. Embong Malang No. 21-31
Surabaya 60261 – Indonesia
T: +62 31 9924 5759

Yogyakarta
Gelanggang Inovasi dan Kreativitas
Universitas Gadjah Mada
Jl. Pancasila No. 1 (Bundaran UGM), Blimbingsari
Daerah Istimewa Yogyakarta 55281
Indonesia
T: +62 274 5059 188

www.pwc.com/id