KPMG

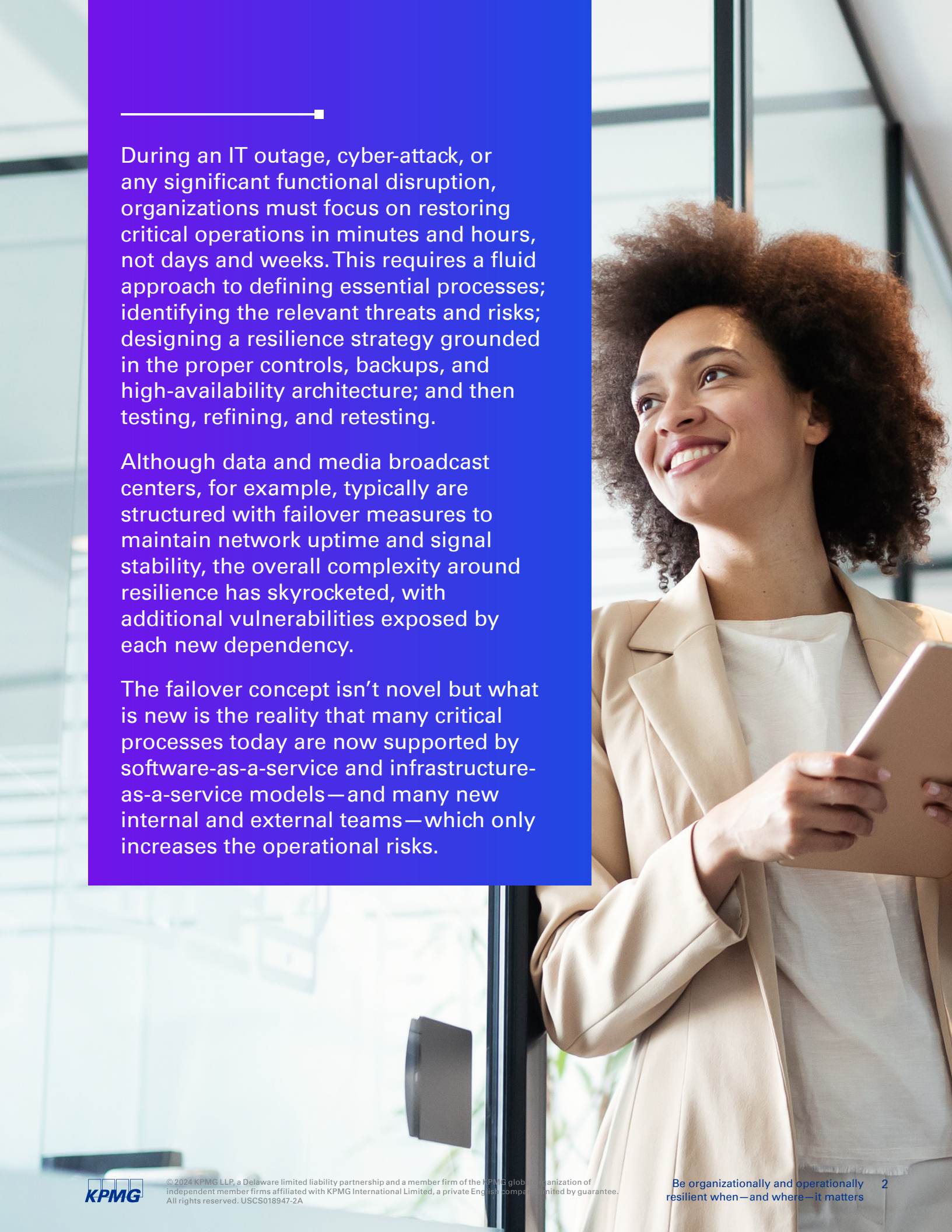
Be organizationally and operationally resilient when—and where—it matters

August 2024

During an IT outage, cyber-attack, or any significant functional disruption, organizations must focus on restoring critical operations in minutes and hours, not days and weeks. This requires a fluid approach to defining essential processes; identifying the relevant threats and risks; designing a resilience strategy grounded in the proper controls, backups, and high-availability architecture; and then testing, refining, and retesting.

Although data and media broadcast centers, for example, typically are structured with failover measures to maintain network uptime and signal stability, the overall complexity around resilience has skyrocketed, with additional vulnerabilities exposed by each new dependency.

The failover concept isn't novel but what is new is the reality that many critical processes today are now supported by software-as-a-service and infrastructure-as-a-service models—and many new internal and external teams—which only increases the operational risks.



Three key themes—Are they on your radar?

In today's volatile environment, resilience has become a key theme for organizations large and small, particularly those across vital infrastructure sectors such as energy and power, transportation, and healthcare.

We encourage CIOs, CFOs, COOs, and CISOs to focus on staying ahead of potential disruptions and build preventative controls across three key areas:

IT resilience

Perhaps the most glaring issue is that organizations often don't have an adequate view of the complex dependencies their IT systems have—both internally and externally—on third parties. Modern IT architectures are moving toward smaller, interconnected services that operate in diverse ecosystems. This makes it challenging to understand all the dependencies your system has on external parties and the impacts that can result from faults or outages.

Also, many organizations have not fully considered what they need to do proactively to ensure their IT systems are as resilient as possible. They assume they have a backup plan and sufficient security controls. But what about more general resilience challenges? How do you respond to a major cloud provider outage? What can you do if your edge network or team workstations go down? Do you understand the impacts these disruptions can have on your regulatory compliance, financial position, or overall brand?

As a concept and a mindset, resilience is imperative for maintaining business operational capabilities, preserving customer trust, and reducing the effects of future incidents.

Business continuity

This is about identifying potential threats and anticipating the impact on business operations those threats could have. Business continuity planning positions the organization to prevent, respond to, and recover from a broad array of future operational disruptions. The key outcome is sustaining essential functional and core revenue-generating business processes during an incident.

Where resilience is strategic—focusing on the ability to adapt to and weather disruptive incidents—business continuity highlights the processes and procedures an organization follows to maintain operations *during* an incident. In that sense, it's much less stressful to carry out a resilience exercise before an outage than in the middle, when multiple business areas and tangential stakeholders may be in panic mode.

An effective business continuity management program strengthens the organization's capability to continue the delivery of products and services at predefined acceptable levels.

IT asset management and operations

While an IT disruption carries implications for every part of the enterprise, CIOs in particular have a foundational responsibility to build a resilient technology stack and IT operating model designed to help the organization manage unexpected challenges to business processes.

Ensuring effective software asset management and maintaining the integrity of complete software records within your configuration management database is vital for streamlined IT operations. This provides accurate visibility into software dependencies and versioning, enabling efficient troubleshooting and ultimately promoting enhanced system reliability and availability.

Too many organizations do not regularly test their recovery processes as a means of proving that value chains can be quickly restarted following a disruption. A robust testing routine is the only way to ensure resilience measures that make sense theoretically can truly be relied upon practically.

Mission criticality: Focus on what matters with advance planning

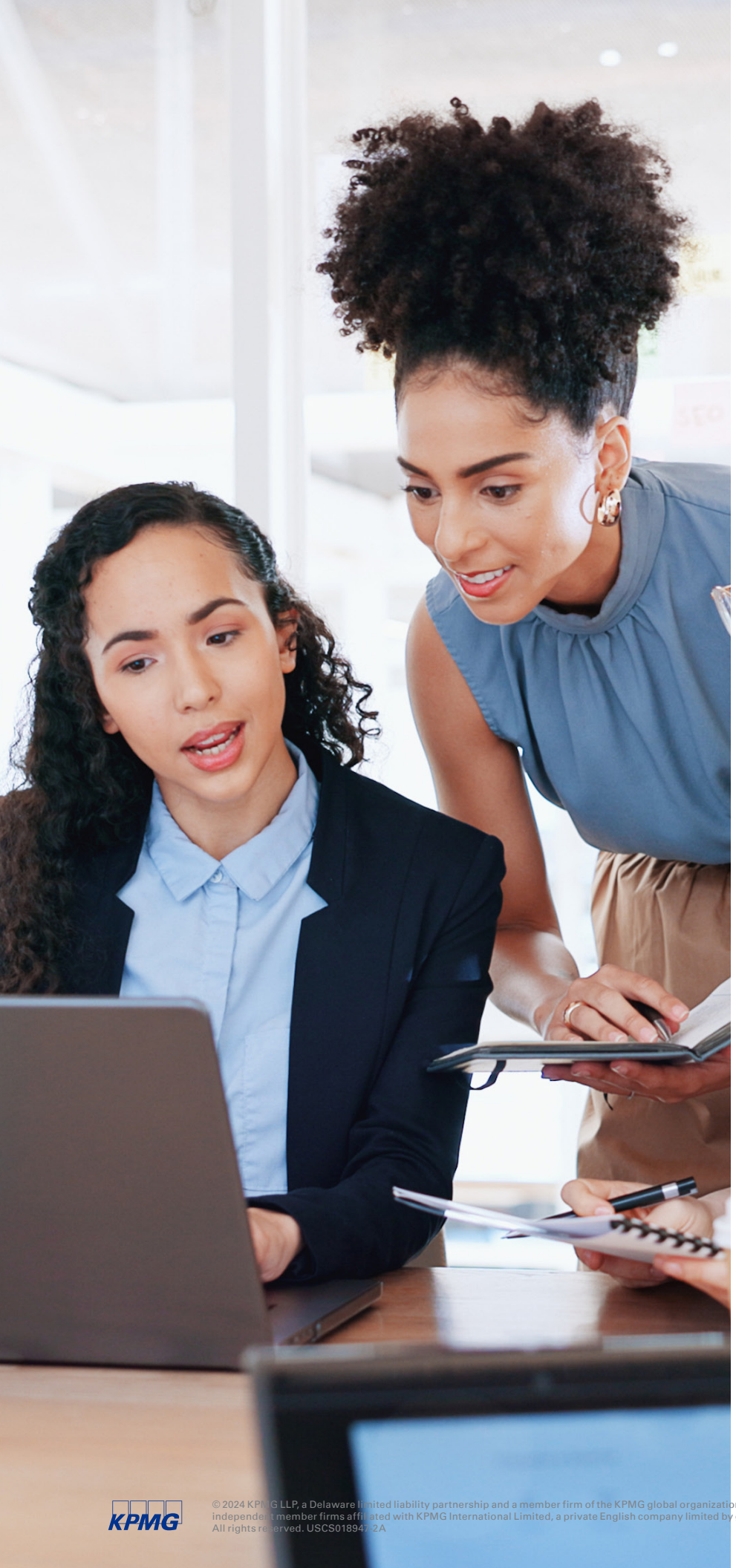
Every organization is unique in what they do and how they do it, but from a resilience perspective, in our view, the first order of business is ensuring people and technology are aligned with the right processes.

It is important to determine in advance which business processes truly are mission-critical and need to be brought back online as soon as possible and understand how these processes function vis-à-vis your technology stack, your vendors, your broad network, and the desired client-facing business outcomes. That perspective facilitates a deeper understanding of the potential risks involved and reveals the building blocks for the appropriate controls.

Structured, scenario-based tabletop exercises are also an important part of preparedness. These exercises expose the strategic choices around how organizations can deal with major disruptive events, such as an errant software update or ransomware incident, and build confidence that leadership is prepared to coordinate response efforts and ultimately lessen the impact on customers, clients, employees, and vendors and suppliers.

We suggest organizations assume an outcomes-based posture when it comes to operational risk and resilience. This transforms a traditional, asset-focused business continuity plan from a periodic exercise to an ongoing long-term tool that utilizes advanced data and analytics to offer a customized line-of-sight that provides decision makers with up-to-date insight into potential risk-reduction strategies that are both fit for purpose and fit for the moment.

Having a written and vetted business continuity plan as a springboard to tangible action is much more effective than brainstorming during an incident.



Position your organization for recovery

In general, organizations' baseline resilience is getting better. But as recent events remind us, there's work to be done. We believe organizations should take steps to embed resilience within IT architecture platforms and the software development and testing lifecycles (SDLC/STLC) from the beginning, rather than bolted on in the end.

Leaders can invest heavily in redundancy, but if they have poor IT asset management, uneven patching practices, inconsistent vendor management, deficient operational processes, and insufficient vulnerability management, then it will be challenging to build sustainable resilience processes.

Following is a list of recommendations leaders should consider as they seek to accelerate recovery times; reduce the impact of incidents on employees, customers, and partners; and aim to structure their resiliency plans to enable—rather than expose—the business.

People

- Connect with your organization's environmental, social, and governance (ESG) team to determine whether they consider organizational resilience a key aspect of their mandate. If not, then work to build awareness of how and why it's important to all three areas of ESG.
- Make resilience an organizational focus and not a paper exercise. It should be viewed as a partnership with cybersecurity, enterprise architecture, business owners, etc.
- Train all key staff about policies and their roles before, during, and after an IT outage.
- Bring a new perspective to the board on what could disrupt the business and what should be done to manage those risks without impacting operations and customer experience.
- Foster organization-wide behaviors and cultural alignment to prioritize what truly matters to the organization in terms of data, services, and infrastructure.
- Encourage a "speak up" culture in which staff are encouraged to and rewarded for identifying possible gaps in resiliency.
- Determine how and where to embed certain resilience-related tasks within the business versus outsourcing to a third-party service provider and monitor those tasks so that they are carried out properly.
- Be practical. Resilience is not as much about getting business partners to do things differently as it is about reframing the conversation across the enterprise to inspire other areas of the organization to infuse the concept of resilience into what they already do.

Process

- Make the knowledge of critical business processes—and the technology and vendor dependencies related to those processes—a foundational element of the organization's resilience plan.
- Define your initial vision and strategy for automation. Consider your short- and long-term resilience objectives, how those goals align with the organization's business priorities, and determine the type of protections those shared objectives require.
- Record IT systems, including business and technical services and associated interconnectivity and dependency on IT assets, in the approved IT system inventory prior to production use.
- Develop robust recovery and help desk processes that are capable of handling spikes in activity.
- Embed resilience in SDLC and other technology change processes and accelerate roll forward activities.
- Enhance transparency to build trust across global supply chains. Rather than treating third-, fourth-, and even fifth-party supplier relationships solely as transactional and contractual (which they are); approach them as an extension of your ecosystem.
- Take a risk-based approach to assessing third-party processes rather than a blanket approach to different suppliers that provide diverse services. Consider onsite audits of third-party partners.
- Encourage crowdsourcing of intelligence and sharing both within your organization and with trusted third parties.

Data and technology

- Develop failover plans for end-user technology as well as servers, based on business priorities and business continuity plans.
- Quantify the risk of those failover plans relative to potential business interruption and the cost. Don't assume failover equates to 100 percent of service—often it does not.
- Focus your data resilience program on your data requirements and loss-acceptability metrics (eg., how much data are you comfortable losing—one hour, one day, one week?).This should dovetail with your failover strategy.
- Identify what data the organization has centrally accessible and define an automated continuous controls monitoring plan to drive efficiencies across all three lines of defense.
- Know where critical data—both structured and unstructured—resides across the organization, as well as how and where it is shared with third-party partners.
- Determine what tools to build versus acquire and understand how supply chain partners are automating to strengthen trust between the organizations and leverage that learning where appropriate.
- Explore more agile and interoperable identity systems to facilitate a robust identity ecosystem.

Regulatory

- Become conversant with the provisions of the Digital Operational Resilience Act (DORA). A crucial component of the European Union Commission's digital financial package that went into effect in January 2023, DORA aims to enhance the digital resilience of the European financial market. Its primary objective is to ensure that financial market participants can maintain safe and reliable operations, even in the face of significant disruptions in information and communication technology. Companies affected by this regulation have been granted a transition period until January 2025 to achieve full compliance. Be conceptually prepared should a version of DORA come to the US.
- Sharpen your global regulatory intelligence around resilience and cybersecurity with a focus on timely compliance and reporting.
- Keep track of and remain familiar with ever-increasing and evolving regulations and the relevant requirements.
- Align your artificial intelligence (AI) framework with current standards and develop solid AI governance by aligning the priorities of the various business leaders in the organization and gaining cross-functional support from those with a vested interest in the success of AI.
- Maintain an understanding of the global regulatory landscape, specifically an understanding of the relevant rules at a granular, jurisdictional level.
- Keep your approach to identity flexible to enable your architecture to facilitate the inclusion of emerging technologies into the network access process as expeditiously as possible.

How KPMG can help

KPMG has experience across the continuum—from the boardroom to the data center. In addition to assessing your organization's ability to remain resilient and aligning those activities with your business priorities, KPMG professionals can help you build resilience of critical processes, develop advanced digital solutions, advise on the implementation and monitoring of ongoing risks, and help you respond effectively to incidents. No matter where you are in your resilience journey, KPMG can help you reach your destination efficiently and effectively.

Our professionals know how to apply leading resilience practices and build new ones as needed. Our progressive approach includes a transparent plan for the delivery of relevant tools, so you can expect to work with people who understand your business and your technology.

Whether you're entering a new market, launching products and services, or interacting with customers in a new way, KPMG professionals can help you anticipate issues and move more efficiently and confidently. Our people bring a combination of technological experience, business perspective, and creativity to the process of helping you protect your network and build stakeholder trust.

Relevant services include:

- Operational Resilience
- IT Asset Management
- Cyber Security
- Enterprise Architecture
- Network Security
- Business Process Optimization
- KPMG Powered Enterprise Resilience

Connect with us

David Tarabocchia
Principal, CIO Advisory
E: dtarabocchia@kpmg.com

Mark Solomon
Managing Director, CIO Advisory
E: marksolomon@kpmg.com

David Woodson
Director, CIO Advisory
E: dwoodson@kpmg.com

Jason Haward-Grau
Principal, Cyber Security Services
E: jhawardgrau@kpmg.com

Vivek Mehta
Principal, Technology Risk
E: vivekmehta@kpmg.com

Sagar Mhaskar
Director, CIO Advisory
E: smhaskar@kpmg.com

KPMG. Make the Difference.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: **kpmg.com**