KPMG

Building a resilient technology stack and operating model

kpmg.com

Consistent preparation is key

Safeguarding business continuity has become significantly more complex and difficult now that supply chains stretch around the globe, and the digital revolution requires companies to commit to consistent and ongoing preparation for both physical and technology disruptions.

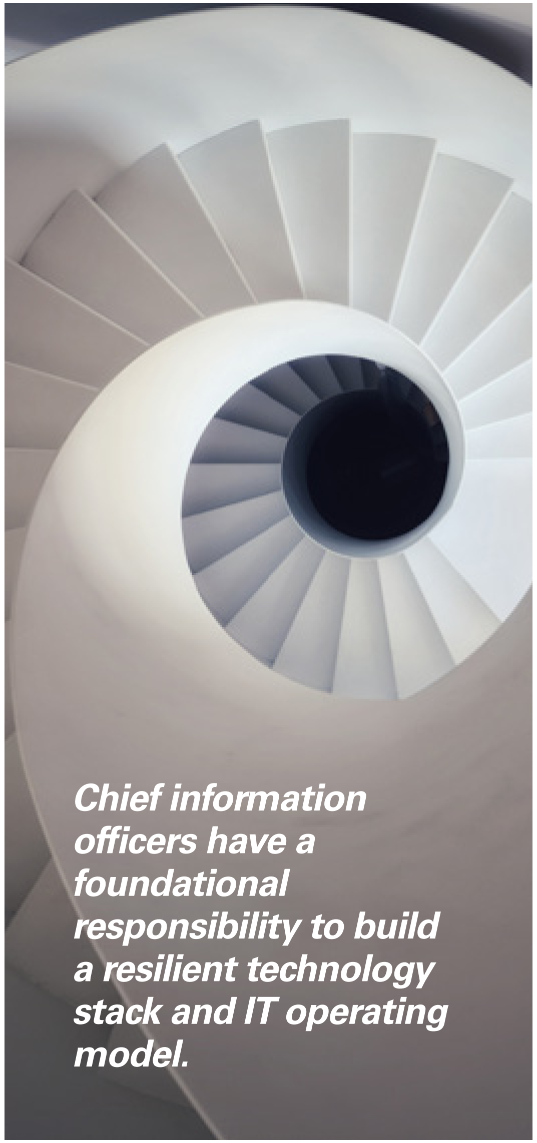
Today, the ability to identify and respond to unexpected events and disruptions has become increasingly critical across so many dimensions—reputational, financial, regulatory, legal, health, and safety—that it has risen at many organizations to the top of the corporate agenda.

While there are implications for every part of the enterprise, chief information officers have a foundational responsibility to build a resilient technology stack and IT operating model that can help their organization weather unexpected challenges to business continuity.

Easier said than done, of course, but following are seven concrete steps CIOs can take to make sure their tech stack and IT operating model have the resilience needed to perform under duress:

01 **Start by identifying those services and systems** critical to the business and its customers—as well as the people, locations, and vendors that support those services and systems.

02 **With that map in hand, identify and catalogue** all of the data elements, both at rest and in transit, required to keep the organization's critical business operations humming.



Chief information officers have a foundational responsibility to build a resilient technology stack and IT operating model.

2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

03

Plan for complex and sophisticated attacks. Plan, for example, for a ransomware attack in which data security is threatened, and large-scale recovery and restoration efforts may be needed, or for geopolitical developments that could disrupt a key vendor's ability to deliver on its service level agreements.

04

In developing the IT operating model, ensure that resilience is a foundational consideration during the planning, development, delivery, enhancement, and maintenance of any new applications or systems introduced into the technology stack. This model should bring diverse parts of the enterprise—business, legal, risk and compliance, and all aspects of the IT organization, including cybersecurity—together with well-defined roles and responsibilities and clear handoff and escalation paths.

05

Digitize and automate resilience processes through contemporary, market-leading platforms to improve recovery consistency and efficiency. For example, the IT organization may want to standardize recovery plan documentation and store it in a location or system accessible during an outage. Automate recovery testing, infrastructure, and application recovery using scripting and tools. Use artificial intelligence for anomaly monitoring and detection.

06

Regularly test resilience and recovery systems and processes to validate they can be relied upon. Training exercises should be frequent and robust, escalating in complexity as the organization matures, and scenario driven—and not always announced ahead of time.

07

Include resilience requirements in the company's vendor management program, and hold critical vendors, including cloud service providers, to a higher standard of availability and recovery than less critical partners.

The IT organization may want to standardize recovery plan documentation and store it in a location or system accessible during an outage.

2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

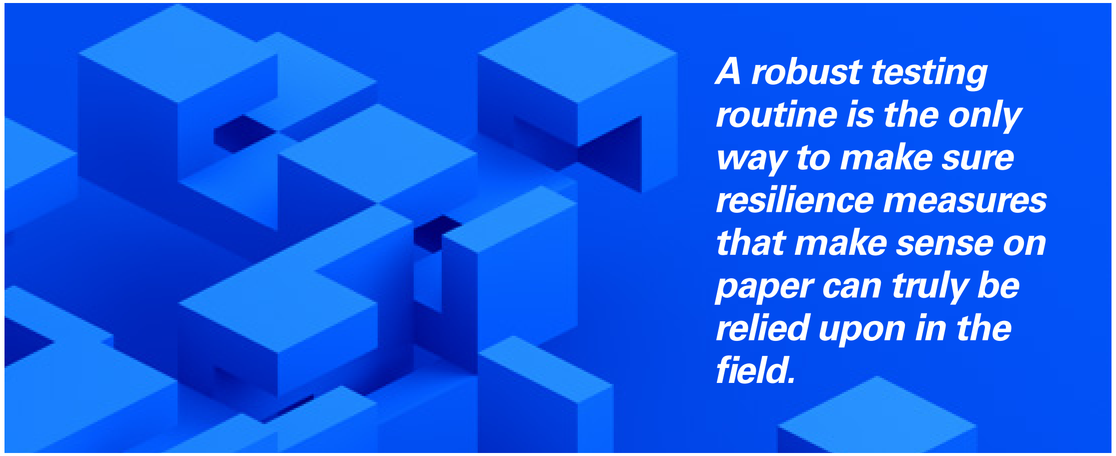
As we work with clients across industries, we see a number of areas where organizations often stumble in their efforts to build a resilient technology stack and IT operating model.

One common mistake is to treat the challenge solely as a technology problem. By bringing their peers in the business into the planning process, CIOs can develop a resilience strategy that protects what is most important to the enterprise—without veering down digital alleys and byways that can sap resources and momentum. This at times may include the use of new systems or applications on an interim basis that require additional IT considerations.

In the same vein, organizations sometimes look to a specific tool as the solution to resilience. But individual tools—especially off-the-shelf varieties that can't be highly tailored to your organization—may struggle to deliver what your business needs. Indeed, retrofitting existing platforms with bolt-on tools often fails to yield optimal results. CIOs can sidestep this problem by performing requirements gathering for a tool, ranking features from "must have" to "good to have" to "expendable," and then performing a market scan to identify the tools that can best meet those requirements.

Finally, too many organizations are not testing their recovery processes with enough rigor to prove that value chains can be quickly restarted following a disruption. A robust testing routine is the only way to make sure resilience measures that make sense on paper can truly be relied upon in the field.

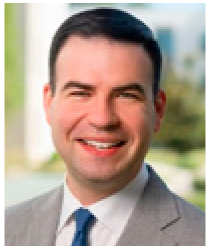
If you're concerned that your organization's tech stack and IT operating model aren't sufficiently resilient, take some time over the next few months to get answers. Define the risks to your business and the gaps in your current capabilities. Then, start building and executing against a delivery strategy to reduce resilience risk to an acceptable level.



A robust testing routine is the only way to make sure resilience measures that make sense on paper can truly be relied upon in the field.

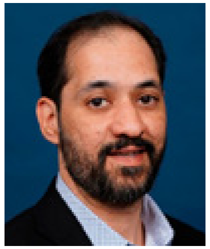
2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

At KPMG, we apply our extensive experience and deep domain knowledge every day to helping CIOs build modern IT organizations fit for tomorrow. To learn more about how we could help your business create a more resilient technology stack and IT operating model, please contact:



David Tarabocchia
Principal, U.S. IT Strategy
Consulting Leader
813-301-2104
dtarabocchia@kpmg.com

Paul Baguley
Principal, CIO Advisory
408-367-7608
paulbaguley@kpmg.com



Sagar Mhaskar
Director, CIO Advisory
804-782-4249
smhaskar@kpmg.com

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

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

2022 KPMG LLP, a Delaware limited liability partnership and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

kpmg.com/socialmedia