# Organizational Resilience in 2024

Adapt in times of uncertainty and agility

Dr. Alea Fairchild, Constantia Institute srl

# Drivers for Organizational Resilience

In current economic conditions, organizations need to leverage their infrastructure to its fullest effect. And that is both land, labor and capital. One of the two main themes I am looking at right now is organizational resilience and how organizations address that need for agility.

So what is operational resilience? And why am I calling it organizational resilience instead?

Operational resilience starts from the perspective of protecting an organization's key business assets (both products and services) and, importantly, begins from the assumption that these assets WILL be disrupted at some point in the future. Operational resilience is a key issue that should be strategically led by boards and senior management.

We take that term a step further, given what we have seen in the last two years, to describe organizational resilience. Because it also involves the workforce, supply chain partners and communication platforms.

There are several key elements that contribute to organizational resilience. These include having robust and flexible plans in place for responding to disruptions, having a diverse range of resources and strategies available, and promoting a culture of continuous learning and improvement.

Effective communication is also critical for organizational resilience, as it allows for the rapid sharing of information and coordination of efforts during times of crisis. It is important for organizations to have clear channels of communication in place and to regularly test and review their communication systems to ensure they are effective.

# Adapting from Disruption

Another key aspect of organizational resilience is the ability to adapt and learn from disruptions. This involves regularly reviewing and refining processes and procedures, as well as seeking out opportunities for innovation and improvement.

Overall, the concept of organizational resilience is about preparing for and effectively responding to disruptions or challenges, in order to ensure the long-term viability and success of the organization.

One aspect of organizational resilience is a flexible and engaged workforce. We have seen staffing shortages and the battle for talent impact the agility of many organizations in recent years. Changing patterns in the employment and workforce landscape mean that employers and employees must adapt their relationships to make workplaces productive and safe environments for all. Work-force centric operations are crucial for organizations to attract and retain talent. And workspaces need to address the diverse needs of the employees and their customers, so another need for agility and ability to pivot.

Another aspect of organizational resilience is communication, more specifically the organizational reliance on the platforms of others to communicate. Outages on social media or other communications tools silences the ability to engage. Ransomware holding information hostage has a similar effect.

# Resilience in the Org Chart

There are many aspects to organizational resilience that go beyond operational deployment.

So where should this view of resilience sit in the organization? That's a good question. Companies will have to decide where OR sits in their organization. This will vary according to the company and its attitude. Will they have a Chief Resilience Officer, or will resilience be a part of Risk, Information Security or some other function? Most companies already have Business Continuity Planning, which tells them how they will respond to a crisis and get back to where they were before. While OR is about much more fundamental threats than that, we could see an evolution of this role in the next 18 months.

In this regard, what have we learned from the pandemic? Not necessarily enough. Supply chains, cyber resilience from ransomware and other bad actors, staff shortages, health and hygiene issues – the risks to operational activities can feel endless.

# Navigating the 'New Normal'

Employers and employees are both juggling what their new normal looks like, and how to integrate pandemic-learned behaviors and activities into a post-pandemic world. An uptake in digital tools allowing for remote work, the creation and support of virtual company cultures, and an internal focus on tools for employee engagement and satisfaction are all examples of these pandemic-based approaches that also need operational resilience built into them.

Heading towards 2025, I see different levels of preparedness in terms of operational resilience across the globe. It can be seen as most advanced in the UK and just starting in the rest of Europe. The EU has applied regulatory pressure in the financial sector with its Digital Operational Resilience Act (DORA). DORA is a “game changer” that will push Financial Services firms to fully understand how their ICT, operational resilience, cyber and TPRM practices affect the resilience of their most critical functions as well as develop entirely new operational resilience capabilities.

It’s important for businesses to remember that complying with regulations doesn’t mean they’re truly resilient. Even if it puts you on the right path, simple compliance shouldn’t be seen as the final destination. And if all you’re focused on is meeting your obligations, it’s difficult to see the bigger picture. That’s our challenge for the next few years.

In terms of the view of resilience in the organization, what are the elements that need to be addressed?

# Building Agility

In my opinion, the main one is organizational agility. Resilience needs to be thought of not just as an exercise in compliance, but as a guiding principle for constantly improving and updating operations. With appropriate risk messaging from business leaders, an organizational resilience mindset should be shared by all personnel, from C-suite to IT professionals and built into the onboard processes as well.

Let’s discuss metrics.

The ability of organizations to measure and track the impact of changes--as well as changes in trends over time--are important tools to effectively manage both resilience and agility.

Like in cyber resiliency, organizations should be identifying and assessing resilience measures by defining their risks by vulnerabilities or by value. This process should include investigating the ramifications of partners' operational resilience—or lack thereof.

What kind of questions should be addressed?

1. How resilient is my organization? And how are we defining this and for what stakeholders?
2. Have our processes, resources and assets made us more resilient?
3. What should be measured to determine if performance objectives for operational

Finally, what initial actions can an organization take to get started addressing this? Two come to mind.

## Take Action: Identify Interdependencies

Identify what chain reactions might result from certain events or changes. Make a thorough inventory of connections and interdependencies between the organization and its partners, vendors, customers, workers, support organizations, departments, and business units.

Figure out risk profiles and what kind of risk tolerance the organization can handle.

Organizations should act on recommended mitigation measures. For example, establishing IT systems resilience might require having more backup resources or additional network redundancy. Regarding vendor or partner risk management, resilience agreements may be needed to guide responses in the event of a crisis or disruption.

## Summary - The Role of the CIO

Organizational resilience refers to the ability of a company or organization to adapt and recover from disruptions, whether they are external or internal. This can include things like natural disasters, economic downturns, or technological failures.

Having a strong level of organizational resilience means being able to anticipate and prepare for potential disruptions, as well as having the resources and processes in place to quickly respond and recover when disruptions do occur. This can involve things like having backup systems or redundant infrastructure in place, as well as having a culture and leadership that encourages and supports adaptability and risk management.

CIO level managers play a key role in building organizational resilience, as they are responsible for managing the technology and systems that enable the organization to function. This includes implementing robust security measures to protect against cyber threats, as well as developing contingency plans for when systems go down. CIOs can also work with other departments to ensure that the organization has the flexibility and agility to pivot and respond to changing circumstances.

Overall, having a high level of organizational resilience allows a company to weather the storms of change and continue operating effectively, even in times of crisis.

# Dr. Alea Fairchild

Dr. Alea Fairchild is a Research Fellow at The Constantia Institute, which is a Brussels-based technology policy think-tank, focusing on innovation and technological advances and their impact on industry and society.  As a technology commentator she has a broad presence both in the traditional media and extensively online. Alea covers the convergence of technology in the cloud, mobile and social spaces and she helps global enterprises understand the competitive marketplace and to profit from digital process redesign.