

REPRINT

R&C risk & compliance

DEFINING THE FUTURE OF OPERATIONAL RESILIENCE

REPRINTED FROM:
RISK & COMPLIANCE MAGAZINE
APR-JUN 2021 ISSUE



www.riskandcompliancemagazine.com

Visit the website to request
a free copy of the full e-magazine

PERSPECTIVES

DEFINING THE FUTURE OF OPERATIONAL RESILIENCE

BY **PAUL JOHNS**
> SAI GLOBAL

Traditionally, business continuity and operational risk have operated as two separate silos within organisations. Is this the best method for mitigating risk in a world where business is changing by the second? Industry expert Michael Rasmussen says the answer to that question was made abundantly clear in 2020 – embedding business continuity more deeply in risk management is the best strategy to achieve operational resilience.

However, few companies are prepared to handle the risks that emerged in 2020 unless they were practicing the integrated, holistic strategies inherent in an operationally resilient approach.

Business vs. operational resilience

There is a common misconception that operational resilience is the same as business resilience, according to Mr Rasmussen. Business resilience is more of an umbrella term that considers an organisation's overall strategy, liquidity and the ability of operations to continue amid changing risks. It asks whether the strategy is diversified, agile and resilient enough for the business to achieve its goals.

Operational resilience is a key component of business resilience that focuses on internal processes, services, people, systems and relationships — and the events that impact these factors.



2020 showed companies the dangers inherent in keeping continuity, risk management and other critical functions separately siloed in a business.

For many organisations, business continuity focused mainly on IT security disasters. When the global pandemic struck, it became obvious that this limited resiliency did not extend to a health disaster. True resilience requires breaking down

silos, promoting collaboration and embracing accountability.

Accountability and resilience

The regulatory landscape is shifting toward enforcement of accountability, according to Mr Rasmussen. In the UK, for example, the Senior Managers and Certification Regime (SM&CR) is

designed to discourage misconduct by centring accountability as a key position function.

Under the SM&CR, there is a specific management role responsible and accountable for different areas of risk, compliance and controls. If there is wilful wrongdoing, that manager can go to jail or be fined from their personal accounts rather than the company's accounts.

When organisations are pressed to distribute accountability, they tend to do so in a way that enforces operational resilience. They are forced to question things like environmental strategy, social governance and flows of information that guide decision making. These questions, although prompted by a regulatory shift toward accountability, are also essential in improving agility. It is not enough to simply respond to mandates in a cursory manner, says Mr Rasmussen. Companies need to use these opportunities to drive an efficient, effective and safe business for employees, shareholders, third parties and investors.

Building resilience into an organisation

How can companies ensure that resilience is built into the organisation? Mr Rasmussen's advice: you must first define it. The UK Financial Conduct Authority (FCA) defines operational resilience as the ability to prevent, adapt, respond to, recover and

learn from operational disruptions. The US Office of the Comptroller of Currency defines operational resilience as the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard.

“Companies must parse risks and exposures to a granular level and determine how a breakdown in one area cascades through the overall service.”

To align with both these definitions, firms must recognise the interconnectedness of risk and integrate multiple elements of risk management around responding to threats quickly and proactively. “If anything, what we've learned over 2020 and into 2021 is we have to build a risk management strategy that's able to react, respond to and recover from any number of these risks that happen around us,” says Mr Rasmussen.

However, businesses must make sure resiliency-focused changes match company values and goals.

Evaluating impact tolerance is another key step in bolstering resilience. Management must define the company's processes and services and define

how they affect third-party relationships with a clear diagram. How will the company stay within the boundaries of impact tolerances at different times?

According to Mr Rasmussen, organisations must be able to recognise the interconnectedness of risk while also being familiar with individual services, systems or processes within the ecosystem. In other words, the organisation must monitor the forest while also being familiar with each tree. Furthermore, Mr Rasmussen pointed out that “we need to see the leaves and the branches, that it’s not just the tree”. Companies must parse risks and exposures to a granular level and determine how a breakdown in one area cascades through the overall service.

Leadership and community engagement

Operational resilience does not develop at the drop of a hat and is not achieved overnight. “You’ve got to have a project plan on how you’re going to execute and deliver,” says Mr Rasmussen.

The key to nurturing resilience lies in collaboration between the right people in operational risk, business continuity, vendor risk and other roles, such as IT security, compliance and ethics. They must define what resilience means in the context of the business and discuss how to implement it across the organisation.

When building out a strategy, Mr Rasmussen advises companies to conduct a current state assessment, map groups and roles within the organisation and reallocate resources for greater

impact. Then, assess future technology needs and determine resilience metrics in terms of mitigation and response.

With objectives defined, employee engagement should improve agility. Many risk and compliance employees spend 80 percent of their time just on documentation or reconciliation. The right approach can flip that allocation, so the majority of time is spent actually improving risk.

Training employees and engaging them with frequent communication improves accountability and resiliency. By issuing clear directives and streamlining the channels through which key messaging is delivered, companies can ensure employees become critical assets in agility.

As risks shift in size and scope, businesses must be prepared for anything. By executing on an operational resilience roadmap, companies can surmount risk-based barriers to business growth and ensure continued regulatory compliance while adhering to company goals. **RC**



Paul Johns

Executive Vice President

SAI Global

T: +1 (917) 689 5876

E: paul.johns@saiglobal.com