The International COO Community (**iCOOC**)
Industry Paper 2024 - 2025

# Operational Resilience

## COO Perspectives

ARMSTRONG WOLFE™

# Index

# Acknowledgements

With thanks to our members, alliance partners and industry advisors for their contributions

## International COO Community (**iCOOC**) members

- **Sam Ahmed** COO Global Financial Markets
  DBS
- **Khadeeja Bassier** COO
  NinetyOne
- **Chris Dickens** Head of Non-Financial Risk
  MSS | HSBC
- **Loretta Marcoccia** Executive Vice President and Chief Global Operations Officer
  Scotiabank
- **Mark P Matthews** Global Operations Head
  Nomura
- **Mark Price** Co-Chief of Staff & Head of Markets (Middle East) CIB Standard Chartered

## Industry Advisors (Buy Side)

- Martha Fee
- Anil Mangla
- Annabelle Plotkin
- Nikitas Psyllakis
- Rob Scott

## Industry Advisors (Sell Side)

- Randi Abernethy
- Richard Austin
- Toby Billington
- Penny Cagan
- Ed Clementi
- Katy Matvey
- George Nunn
- Rob Wilson

## Industry Advisors (Regulation)

- David Blunt
- Ted MacDonald
- Georgina Philippou

## Alliance Partners

- **Fahreen Kurji** Chief Customer Intelligence Officer
  Behavox
- **Andy Nelson** UK CEO Financial Services
  NTT Data
- **Chris Rigg** Partner
  Global Economics Group
- **Stuart Tootal** Managing Partner
  Matero Consulting
- **Harry Toukalas** Co-Founder and CEO
  Swarm Dynamics
- **General Sir Peter Wall** CEO
  Amicus

# Armstrong Wolfe

## The Power of Collective Ambition

We are dedicated to supporting the worldwide Chief Operating Officer communities of Financial Markets, Banking and Asset Management.

As members of the International COO Community (iCOOC), you are part of a global network working together to address market side, non-proprietary challenges.

Our member hosted breakfasts, dinners and virtual forums are conducted under Chatham House Rule, allowing COOs to investigate and share thoughts and challenges. Core areas of debate are within non-financial risk, operational resilience, first line controls and conduct, regulatory adoption, AI and transformation and leadership.

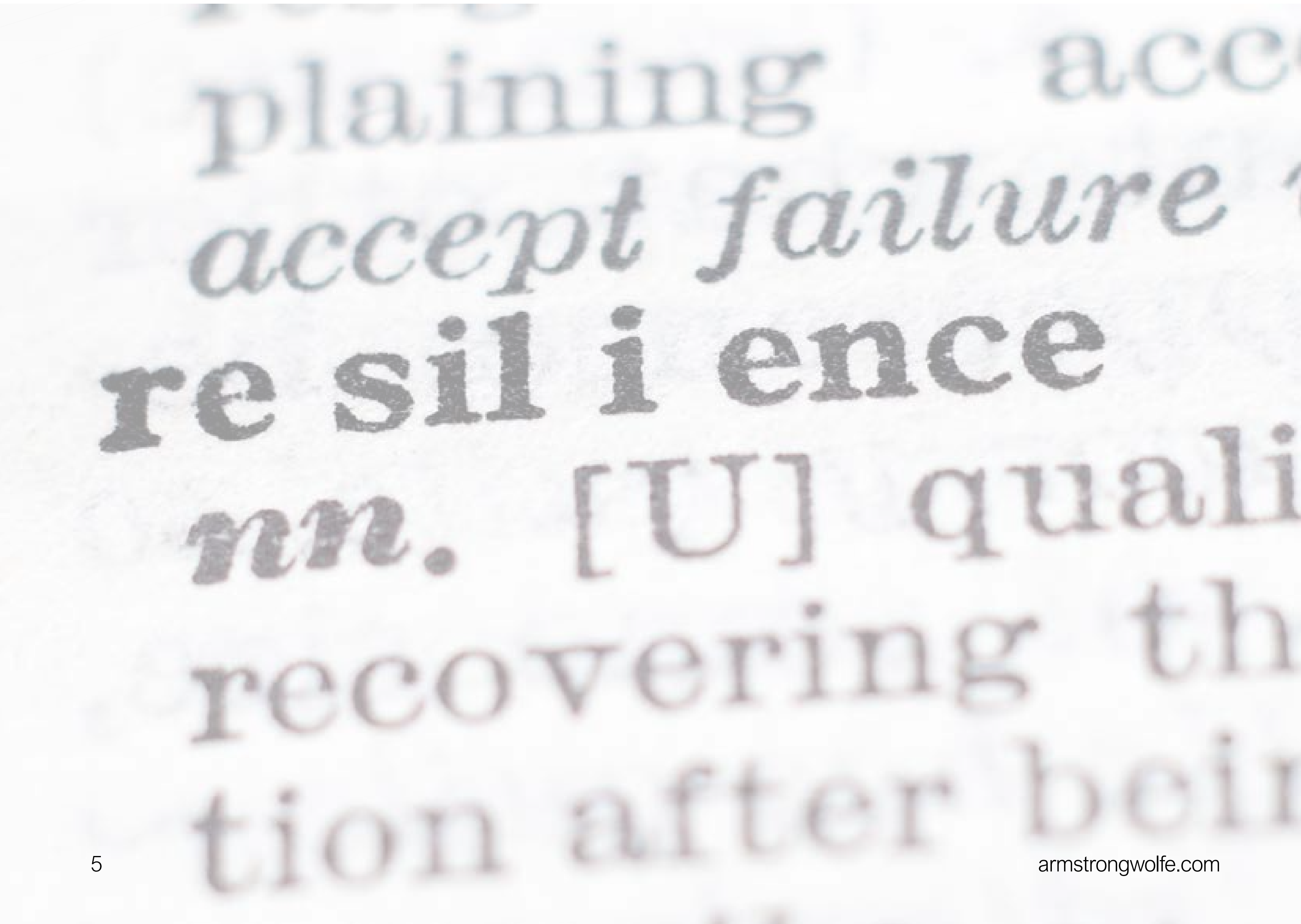
Corporate members engage in our DEI programmes, Ad Centrum and Women in the COO Community (WCOOC), whilst our Leadership and Performance Institute supports developing talent at all levels.

Through these integrated offerings we are the COO's trusted partner.

Join us, contact info@armstrongwolfe.com

# Foreword

**Maurice Evlyn-Bufton**
CEO
Armstrong Wolfe



Cyber | Technology | 3rd Party Vendor

Business Continuity | Crisis Management

# With global regulators adopting differing levels of scrutiny within resiliency, some financial services companies have responded by appointing a global head of operational resilience, invariably reporting to the Chief Technology Officer.

## This is understandable when much of the resiliency risk sits within technology - but importantly - not all of it.

In the UK, the Senior Manager's regime imposed an obligation on the COO, appointed SM24, as the senior executive with responsibility for the operations and technology of the company. This manifested itself with the requirement to establish an operational resilience framework.

The regulatory interim deadline of April 2021 - March 2022 was an initial implementation period, which required the SMF24 to implement all aspects of the policy, except being able to stay within impact tolerances at all times.

We entered the next phase in March 2022, carrying through to March 2025 which is the transitional period whereby firms are required to invest in their ability to remain within their impact tolerances.

This confirmed a focus on cyber security, 3rd party vendor management, technology, and the link into business continuity, all being scenario stress tested.

One COO noted:

> *"These are all established risks, nothing new, but we must now look at them through a nuanced lens, called resiliency. It's become a wrapper around what we already do, where this can lead to a fragmented approach."*

Most argue this fragmented approach can be managed by taking a horizontal view across business activities to test resiliency, some suggest a framework would be better aligned to established non-financial risk taxonomies, providing oversight to meet resiliency requirements.

Change
Agility
Strength
Confidence
Determination
Challenge
Motivation
Endurance
Resilience

Alongside the debate on management and governance, COO feedback suggests there are several topics that supersede governance in their importance:

- **Can we better manage third parties** that are systemic to the industry?
- **Do we have a consistent view** of ‘severe but plausible’?
- **Can we standardise responses** to customer demands with regard to op res assurance?

These are worthy of debate and will be tabled throughout 2024 and 2025 as part of The International COO Community (**iCOOC**) programme of debate. iCOOC will further investigate whether the fragmented approach noted above could lend itself to the design and implementation of an integrated resilience framework.

Key points of discussion will be:

- **The governance of operational resilience**, the marriage and integration of established 1st and 2nd line risk and control functions, the over lapping role of risk committees, and how best to develop, test and provide a non-financial emerging risk and horizon scanning capability.
- **A capability that would partner resiliency,** thus ensuring interoperability and sustainability of the business against the impact of anticipated and unforeseen events.

Within this programme of debate the aim is to evaluate the role of the COO in meeting the demands of operational resilience, define principles for adoption and explore ways in which the community can benefit from cross industry discussion on this market-wide, non-proprietary challenge.

# From the Central Chair

## Opening Remarks

Since 2008 the industry has been through a costly era of regulatory imposition. The multi-jurisdictional nature of regulation and lack of global cohesion has added to this complexity.

> *"Disparate and on occasion competing and conflicting functions have developed in response, implementing controls, and building resilience, be this the 3LoD, operational and enterprise risk, and business continuity management.*
>
> *We appear to be entering a new phase with the emergence of a functional first line nonfictional risk dovetailing with its regulatory sibling operational resilience. This offers an opportunity for simplification and efficiencies to be realised.*
>
> *Whether we can rid ourselves of embedded perspectives and interpretations is the uncertainty that will define if this opportunity is grasped or not"*
> **Global COO Banking & Markets and Head of Operations, New York**

> *"Operational Resilience should not be interpreted as an onerous requirement; it is simply the codification of good business practice and a wrapper around what we already do."*
> **EMEA COO, Global Financial Services and Bank Holding Company, London**

> *"For a COO, SMR is a very helpful piece of regulation. It is a Trojan Horse that has allowed me to take it through the business to get things done, leveraging it is the regulatory imperative related to operational resilience"*
> **CIB COO, International Bank, London**

## Piers Murray

COO

Armstrong Wolfe

# A perspective from Armstrong Wolfe's COO

Piers has over 30 years of industry experience before joining Armstrong Wolfe as its COO. He is the former Global COO Markets, BNY Mellon, was global co-head of listed derivatives and clearing at Deutsche Bank and as a managing director at JP Morgan, worked within OTC interest rate clearing, global credit risk and credit portfolio trading.

Operational Resilience has been defined in multiple ways through the course of viewpoints submitted, and the costs of failure to be operationally resilient have been well described, so I will focus on a couple of less explored areas:

- **The delta between business objectives** and resilience requirements established at a firmwide level
- **The human component of resilience,** including leadership in a crisis, the true value of simulations

## The value of a Risk Appetite Statement (RAS)

For many years banks have been required to document their risk appetite, defined as: The aggregate level and types of risk that an institution is willing to accept, or to avoid, in order to achieve its business objectives.

A firm with multiple business lines must prioritize resources to its most valuable business lines first, on the basis of actual cost to meet the stated RAS objectives plus the opportunity cost associated with not doing so, the latter which comes in the form of quantifiable negative reputational, regulatory and client feedback.

The appropriate place to quantify these risks and the desired outcomes is in the RAS; this document provides a basis for a common understanding across the LoBs and across the firm of the relative prioritization of risks and responses.

In the multi-threat environment we face today with state actors describing "asymmetrical warfare", financial institutions need to plan for multiple concurrent risk events that will test their operational resilience.  The response may require a "crisis cabinet", reallocation of senior resources to lead the response, as well as a prioritization process that is clearly articulated.

An effective RAS lays the foundation for subsequent crisis management, as it will lay out the risks, and give a sense of priorities enabling not just the executive leadership but also rank and file to understand and get behind the firm's response.

## The Human Component & Simulations

Leadership, clarity of thought and communication are all key elements of a response to a crisis. Unfortunately, these events are rarely tested in practice on a firmwide basis, but generally covered in one-off, time and seniority limited exercises, with little consistency in feedback to participants, value attributed by senior management, or solutioning from lessons learned: these tend to happen only after real-life events occur.

Risks identified in the RAS need playbooks, but taking comfort in the existence of playbooks without creating institutional muscle memory through simulation doesn't lay the ground for surviving "first contact."

Senior leadership engagement with cyber, default or other risk simulations has typically waned with time post crisis or post regulation. There was no playbook for banks to deal with the invasion of Ukraine: it took the combination of multiple playbooks simultaneously, BCP, default, cyber, sanctions to respond to that event.

Simulations that were undertaken for each of these playbooks without the participation of the senior leadership wouldn't have helped decision-making process at the exec level without witnessing the process and give and take of the simulations.

This is where some new thinking needs to come in: simulations provide the muscle memory to participants for the engagement model needed to respond to a crisis.

The value builds up over time through alternate scenarios and one up/one down participation. Firms need to expressly value the work put into live simulations, to incentivize participation, to extend learning down into the organization and to keep increasing the challenge provided by the simulation over time.

Well conducted live simulations with active executive management participation are worth significantly more than rote training modules. Bringing third-party vendors into the simulation would be an incrementally positive step that firms can take.

Just as simulations provide internal learnings, public events that create an environment of stress for an organization do the same and need to be accompanied by an increased flow of timely communication for the organization to fully rally to the occasion.

While both political and legal considerations risk curtailing needed words of encouragement to the troops, management needs to find a way to communicate the urgency with which it is responding and expectations of the teams to help manage the portfolio of risks, expected and unexpected, that have surfaced. (These communications are another process than can be tested in an effective simulation.)

Lastly, an effective post-mortem process to every crisis is also vital, as findings need to be acted on and can also provide material for future simulations, creating a virtuous cycle of simulating, upskilling & process improvement all of which contribute to operational resilience.

**"Leadership, clarity of thought and communication are all key elements of a response to a crisis".**

# Perspective

/pər'spektiv/ [countable] a particular attitude towards something; a way of thinking about something; synonym viewpoint.

Oxford Dictionary

# SMF24 Perspective

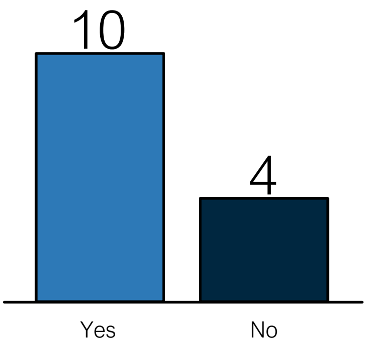
## The COO's regulatory obligation

**SMF24:** The function of having responsibility for the internal operations and technology of a firm.

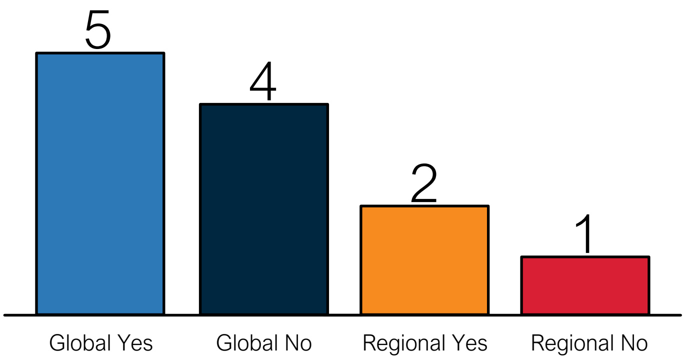
**Split and shared functions**
In certain circumstances, a managing agent may be allowed to have more than one individual responsible for a single SMF where appropriate and justified.

## Insights from a London buy-sell side SMF24 roundtable, June 2024

**1. Do you see the value and need to appoint a Global Head of Operational Resilience?**



**2. Is there a global and/or regional head of Operational Resilience appointed at your company?**



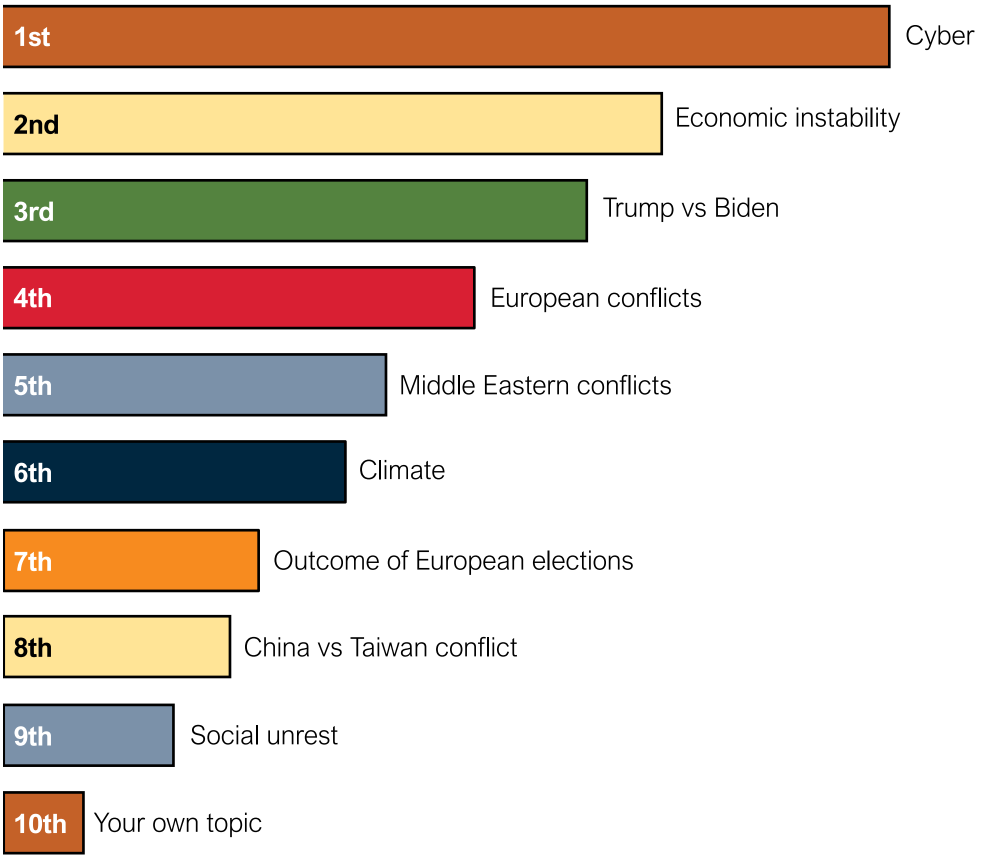
**3. If yes, who do they report into?**

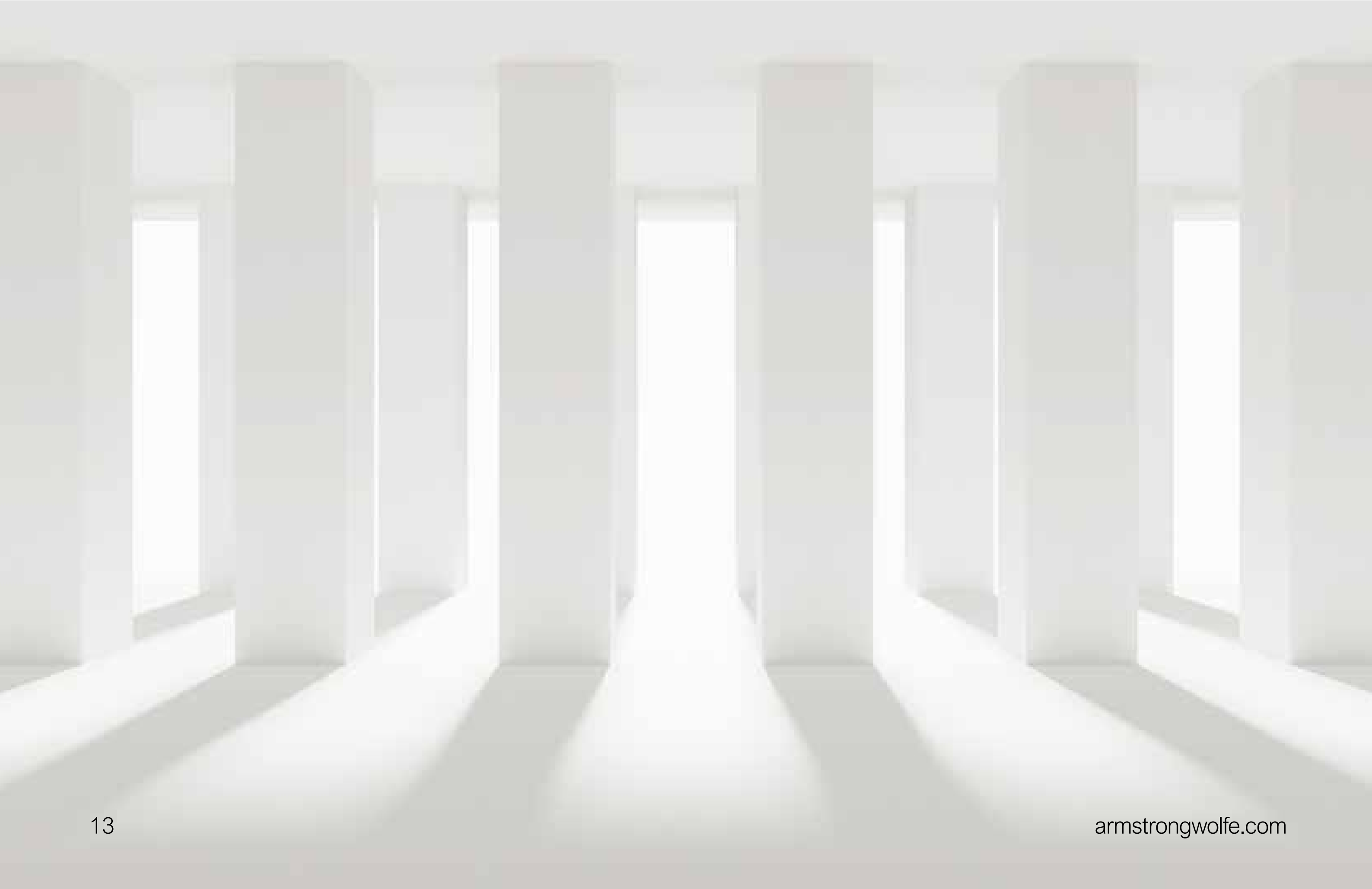
- Head of Controls organisation
- Enterprise Head into Group CAO
- International CAO
- CIB COO, into Group COO
- Group Head of 1st Line Controls
- Head of Technology, Enterprise Operations
- Head of Business Services

**4. What are the principal challenges for the SMF24 in relation to meeting regulatory (FCA) requirements for Operational Resilience?**

- Bandwidth and depth
- Impact tolerances
- Programme vs BAU
- Technology and interconnectivity with consumer duty
- Continuous improvement
- Outsourcing and 'look through'
- Third Party and/or vendor relationships/reliability
- Legal entity complexity and country/jurisdiction risk
- Defining and executing testing scenarios
- Prioritisation and competition with enterprise initiative
- Regions vs business lines vs group inter-relationship
- Resiliency within staffing and corporate culture

5. **1 being the highest, 10 being the lowest, rank the below Non-Financial Risks in order of how impactful they may be over the next 12-24 months**





## Martha Fee

Armstrong Wolfe Advisor

Former SMF24 as COO EMEA & APAC
Northern Trust Asset Management

### The aftermath of COVID-19 has emphasized the criticality of operational resilience in navigating the complexities of today's world.

As regulatory expectations in the UK align with industry efforts, firms are urged to embed resilience into their DNA, from the boardroom to the front lines, to meet the March 31st 2025 deadline.

The overarching principle of operational resilience acknowledges the inevitability of disruptions and underscores the need for proactive preparedness and adaptive measures to safeguard critical business services.

Key principles of an operational resilience framework include board and senior management ownership, identification of critical services, setting impact tolerances, and continuous review and improvement. It's essential to leverage existing frameworks such as Third-Party Risk Management, Change Management, and Business Continuity Planning to integrate operational resilience effectively.

It is clear from UK regulations that the COO and/or CIO with the SMF24 regulated function are accountable for the operational resilience approach, firms' policy standards, and operational models. Equally, executives who own important business services and associated revenues are responsible for addressing vulnerabilities that could breach impact tolerances, necessitating a cohesive approach to governance and oversight.

However, assessing the effectiveness of operational resilience frameworks can be a challenge. Metrics such as program status, tolerance breaches, and vulnerability resolution are invaluable in tracking progress and enhancing resilience.

Drawing from my experience, I would advocate for a structured approach to metrics tracking, focusing on program status, tolerance breaches, and vulnerability resolution.

UK firms have until March 2025 and need to ensure items are being tracked and completed. Consider the following when developing metrics. Tolerance breaches are reportable to the regulator.

- Have you had any, and how many have you reported?
- Have important business services remained within their impact tolerance?
- Have you had any near misses?
- Vulnerability tracking and resolution are crucial. What lessons have you learned and incorporated to enhance your firm's resilience?

These draw upon my own experience as a COO and SMF 24 leveraged when creating structured metrics dashboards, which may resonate with others in the field.

> **"Key principles of an operational resilience framework include board and senior management ownership."**

# WCOOC

## Women in the COO Community

### Supporting, empowering & inspiring the female leadership of tomorrow

Armstrong Wolfe's Women in the COO Community (WCOOC) initiative was established in 2016, and is now globally recognised across New York, Toronto, London, Paris, Hong Kong, and Singapore.

Its purpose is to champion the cause for advancement of women within financial services, focused on the leadership of tomorrow, those that will take the industry forward into the coming age.

Members of our global COO network come together to provide and present on subjects directly related to career management and advancement. We provide this through podcasts, articles, interviews, and events for which we recruit engaging speakers from within and outside the industry. We welcome people of any level of seniority to engage with our agenda.

WCOOC is led by industry professionals, its Chair, Vice Chair, and regional steering groups working together to provide timely and forward-thinking content and thought leadership.

### Our Mission

» To inspire and install ambition and confidence in the female leadership of tomorrow.

» To enlighten tomorrow's leaders on the role of business management and the COO.

» Through this enlightenment to establish the COO as an aspirational career destination.

» To provide networking and confidence building opportunities with industry peers.

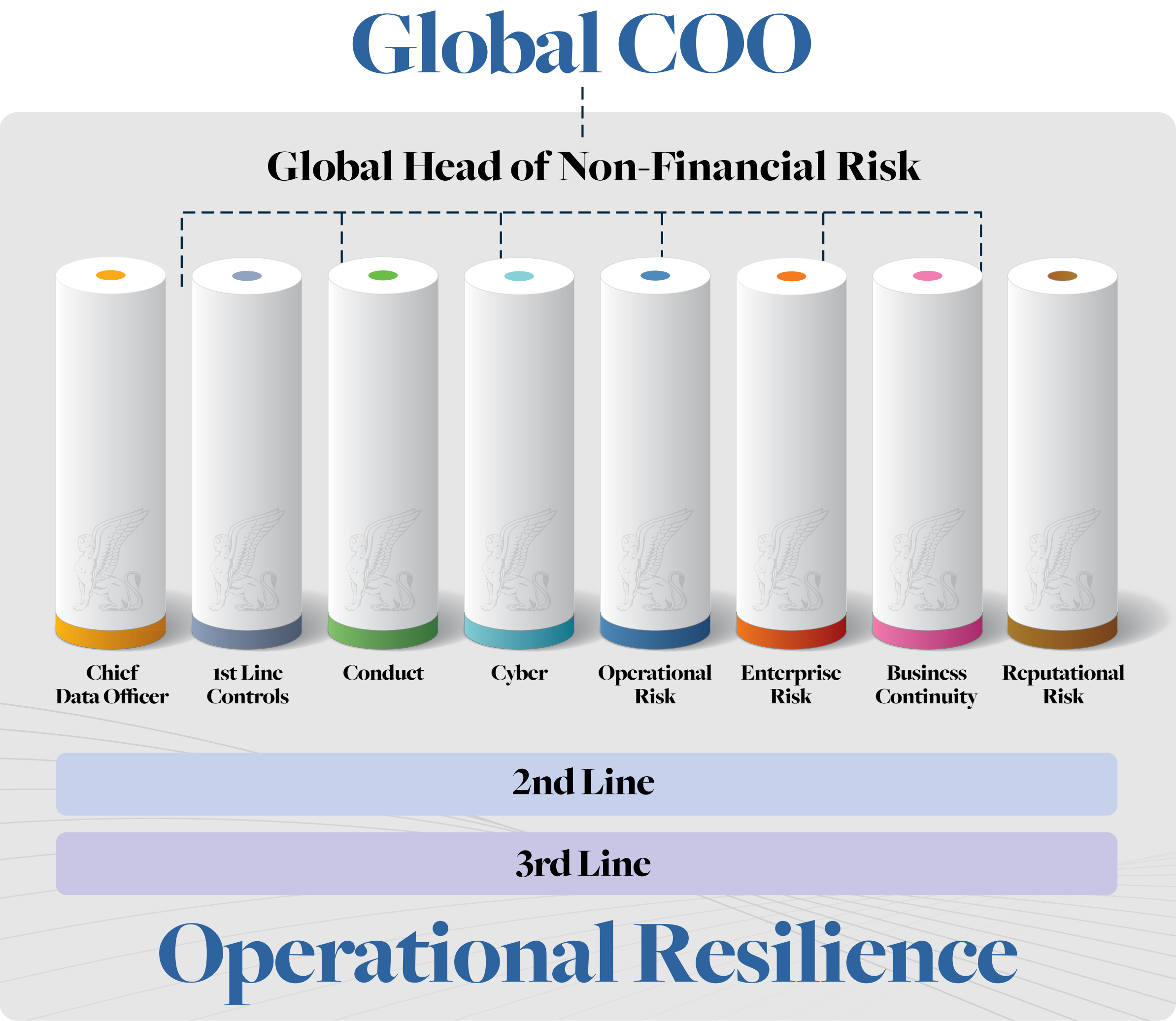
» To provide a forum for cross-industry debate and engagement on market wide challenges.

### Steering Group and Ambassadorship

The Steering and Ambassador Committees are formed from global banks supporting WCOOC and its DE&I initiatives. Their role is to help provide direction and support in the continuation of inclusive leadership for corporate success.

# A fresh perspective on the organisational resilience structure

Some COOs argue it is time to be bold, to take this opportunity of regulatory inquisitiveness to realign and integrate competing functions to deliver a uniformed and more efficient approach to building, governing, and ensuring operational resilience.



Common sense, a bold step or a step too far?

We would be delighted to hear your thoughts: **maurice.evlyn-bufton@armstrongwolfe.com**

# iCOOC Member Perspectives

## Khadeeja Bassier

COO
NinetyOne

1. **The key industry challenges ahead that make operational resilience an imperative business practice**

- More single points of failure
- Digitisation and infrastructural dependency
- AI and the creation of multiple realities makes content verification harder (which increases fraud risk)
- Expectation of immediacy by clients in every point of the value chain

2. **What are the key challenge(s) in establishing operational resilience**

- In a digital first world, true resilience lies in forecasting the unknown unknowns
- Even more rudimentary, the known unknowns are where we have to challenge our existing assumptions
- Operational Resilience is the domain of the entire ecosystem rather than singular teams/people

3. **Who is best to oversee operational reliance**

- I would say it depends on organisational structure
- Independence is important to be seen as legitimate challenge rather than advancing silo'd agendas
- Accountability should be dependent on rollup of these teams and how the recommendations can be implemented

Ninety One

## Chris Dickens

Head of Non-Financial Risk
MSS | HSBC

**For HSBC, it makes sense for Operational Resilience to be business owned given the full response needs input from many functional areas and an understanding of end-to-end flows. Technology has a key role.**

Operational Resilience is a business priority given customer requirements, and the need to manage risk in real time. At the same time, the frequency and sophistication of cyber attacks are increasing.

Banks are investing heavily in their own defences and response capability but also recognise their reliance on third parties.

There is a need for transparency from third parties on their cyber control standards and for Banks to have plans to respond should a critical third party be attacked.

HSBC

An anonymous perception

**As one COO and member offered, who shall remain nameless:** My note reads rather like the infamous Private Frazer of Dad's Army fame when he proclaimed, 'we're doomed all doomed', but genuinely the below is where I am on the topic.

I think there is a lot of intelligent and useful thoughts exchanged but (beyond cyber), my sense is we on the buy-side don't sufficiently talk about these elephants in the room. Nor do the regulators. However, I'd only be comfortable expressing this in a Chatham House environment. I'm concerned my comments may lead the regulator down a road that ends at my office door!

My thoughts on Operational Resilience centre around the third party suppliers, in particular:

- Fund Administrators, e.g. custodians, fund accountants, transfer agents, etc
- IT platforms, most notably BRS's Aladdin

For me If either of these were to fall over, due to a financial calamity or a prolonged cyber event, it is fanciful to imagine any firm could switch within a remotely reasonable timeframe to an alternative provider.

Switches of these types are likely to be 18-36 month projects. I'd be very interested as to the answer firms are giving if asked by the FCA what they would do in the event of either scenario.

I just don't have an answer that doesn't involve the phrase 'wind-down'.

## Mark P Matthews

Global Operations Head
Nomura

**Operational resilience continues to be a strategic imperative for our industry.**

The financial service industry's success in managing through the Covid-19 pandemic should in no way inspire over-confidence in the face of the many challenges likely to emerge in the next 14-36 months.

- Geopolitical tensions in the Middle-East, Europe and Asia
- Shifting political dynamics in Europe and North America potentially
- Increasing cyber risk
- Economic challenges from asynchronous global fiscal and monetary policies
- Evolution of hybrid-working and impact to workforce dynamics and demographics

Given the breadth of challenge, a coordinated approach which brings all parts of an organization together is essential. The risks and resiliency challenge is certainly not limited to Technology, Business or Operations so having a centrally coordinated but federated approach is the only one that provides a level of 'defence-in-depth'.

Operational resilience is not simply a reporting exercise for stakeholders – some risks represent existential threats to organizational survival and have broad industry impact. Recent cyber incidents disrupt business in the short term but reputations for the long term; localized Geopolitical conflict impacts the global supply chain and Covid-19 changed global economic dynamics for decades to come.

Adoption of 'Resilience' as a core part of corporate culture is perhaps the most important focus an organization can have.

NOMURA

## Sam Ahmed

COO Global
Financial Markets
DBS Bank

Assessing the risks to the Global Markets business has been changing over time. Today in the region, we see a lot of emphasis on operational resiliency. This is a result of banks having invested heavily in platforms and digitalisation over the past decade which has borne fruit today with respect to experiencing healthy client adoption and increased volumes for the new digital channels.

With an increased migration of financial markets activities towards digital/electronic venues and platforms, there is a growing focus to ensure these new channels are resilient in face of system disruptions and cyber threats. As a consequence, there is a lot more scrutiny of vendor technology, third party service providers, data centres, together with how vendors are sourced, procured and onboarded.

New assessment standards for any technology implementation associated with new business initiatives are being put in place and separately contingency planning on system disruption are being included as a part of BCP exercises with independent audits ensuring quality assurance and testing being conducted. This is all a part of ensuring banks are thorough with their operational resilience in preparing for unintended outcomes.

## Mark Price

CIB Co-Chief of Staff
& Head of Markets
(Middle East)
Standard Chartered

Oscar Wilde said “To expect the unexpected shows a thoroughly modern intellect”, which I think I a very fitting way to consider the myriad demands, being truly Operationally Resilient requires.

I understood this fully one day, when the Uninterruptible Power Supply that provided the back-up power in the case of a power-cut, caught fire in our main Deutsche Bank building in London, knocking out all of the trading floors.

After that, I learnt that being ‘Operationally Resilient’, means asking “What could go wrong?” across all aspects of business, not just FO or COO, but those oft-forgotten areas such as Property, Procurement etc.

All areas should review their own plans to ensure that they are prepared; that they ‘expect the unexpected’. However, I would still advocate that the COO, with the innate curiosity the role requires, is best placed to coordinate such a review with the right level of independent challenge and scepticism.”

## Loretta Marcoccia

Executive Vice President and Chief Global Operations Officer
Scotiabank

> *Would you be able to offer your thoughts on what you see as the key industry challenges ahead that make operational resilience an imperative business practice?*

Currently, there is regulatory focus across the globe on operational resilience. Organizations are being benchmarked on operational resilience as an imperative business practice, including horizontal reviews on specific incidents that may have taken place. There is also an increase in cyber and fraud disruption, and it is imperative for firms to proactively plan for every eventuality.

Around the world, regulators are making a clear link between operational resilience and liquidity risk, and the standards are being raised by some recent examples at global organizations.

> *What are the key challenge(s) in establishing operational resilience?*

Establishing operational resilience is multi-threaded. It pulls together many areas of the organization that may have historically existed in silos. This includes Business Continuity Planning, Cyber Security/Fraud, IT Risk, HR, and more.

At the same time, there are differing global frameworks. Regulators across the globe are at different stages of maturity in their thinking around operational resilience. It is helpful and important for organizations to converge even more around certain global standards for consistency of terminology and documentation.

It is more important than ever to plan for the 'unknown'. But it is also imperative to plan for the 'unknown' that could impact the industry collectively.

> *There is debate on who is best to oversee operational reliance: some saying technology, some say the COO, some say there is no need for a single point of oversight as operational resilience is simply a regulated wrapper around what we already do. Thoughts?*

Who is best to oversee operation resilience is an ongoing debate. Regulators have clearly stated that the business owns operational resilience and therefore the 1st line needs an owner for operational resilience to drive standards for the organization.

The approach in the industry is mixed, where some have converged on a 1st line owner, others continue to have a 2nd line framework and then business owners in each division.

Scotiabank®

**"The oversight of operational resilience will be an ongoing debate based on what the regulators and organizations believe is best to protect clients and businesses."**

# Perspectives from the Buy side

# Anil Mangla

Armstrong Wolfe Advisor

Former Global Head of Operations Sera Global (Brookfield PortCo); BlackRock and Barclays

For me, operational resilience requirements are here to stay, and demand will only increase, not just from regulators, but also stakeholders such as investors, clients and strategic partners and over time, resilience requirements will intertwine across the entire business platform.

Therefore, organisations should focus on designing and implementing a framework that expands past operations and one that is efficient, cost-effective, transparent and compliant. Continuous refinements and improvements are key as an organisation progresses on its journey, but these will only be temporary until resilience management becomes part of the organisation's DNA. Demonstrating adherence through reports and dashboards is likely to be a much more challenging task.

Solutions need to be easy to adopt, flexible and scalable. Organisations need to be careful and not rely on legacy systems and processes as they risk not being able to adapt to evolving requirements; not benefit from leveraging technology in the right way and spending operating capital on the wrong areas. **Successful implementation will require a balance between quick wins and building a strong platform for the future.**

For many small to midsize organisations, the bulk of this work will most likely be completed via a 3rd party partner and so robust approaches to partner selection and the resulting oversight and governance model is critical.

However, I believe getting Operational Resiliency correct presents organisations a chance to gain some form of competitive advantage, drive revenue growth, manage resources and costs.

Additionally, resilience can be used as an 'indicator' to demonstrate an organisation's health so can positively promote brand perception, client trust and loyalty. In my mind, the following are notable areas for discussion:

## 1. Role of the COO

**COOs are potentially best placed to oversee resilience.**

- Technology (Cybersecurity, Data Protection) is currently most prominent but over time resilience requirements will increase across other risk areas be that business strategy & performance, finance, regulation or other non-financial risks (climate, geopolitical, DEI etc.)
- COOs are well versed in effective oversight and governance; developing and executing operational roadmaps and incorporating ongoing improvements as well as 3rd party partner selection and management.
- COOs are often involved in developing value creation plans for revenue and profit growth and so potentially have a broader view of what is happening and what is forthcoming or changing which can be factored for.
- COOs are a key business conduit and/or the 'right hand' to leadership and so by operating with a partnership mindset, can work seamlessly with other key functional partners such as CTOs, CROs, CCOs and CFOs to ensure everything is captured and accounted for.

## 2. Board Leadership & Organisational Culture

**Board Leadership:** Play a critical role in embedding the right framework and ensuring everyone is engaged and aligned through clear communication, promotion of a risk-aware culture and ensure the right development and training programs are in place.

They need to have a willingness to understand what operational resiliency means; what are the expected standards; what has been designed and the ramifications of getting it wrong (not just financial implications but reputational; regulatory; operational because of increased scrutiny, distractions & remedial actions etc.)

- Align resilience plans to strategic vision, business objectives, culture & values.
- Ensure consistent approach across all the organisation with clear deliverables and accountability.
- Accept this will take time and not just about getting items 'ticked off'.
- Allocate talented individuals who can excel and deliver ambiguous and complex initiatives.
- Support the transformation from being a 'we must do this' to 'how do we turn this into a business enabling opportunity'.
- Conduct regular reviews to ensure the resilience program is 'on track' and future / emerging risks are being accounted for. Insist this is a standing agenda item on any OpCo type committee.
- Should expect this of the firms and organisations that they are also invested in (e.g. portfolio companies)
- Investigate the opportunity to partner with industry peers and form consortiums to collectively develop industry-wide solutions.

**Taking all the above into consideration will hopefully lead to more informed deployment of resources and capital.**

## 3. Artificial Intelligence

Needs to be used in a focused and targeted manner. However, many people don't understand AI and fear it (e.g. AI will take over my job) and so that needs to be factored in to avoid roadblocks and disruption; people are still essential and instrumental in developing the right holistic resilience platform. Areas that could benefit from AI include:

- **Reporting** (Backward and Forward looking).
  - **Wide audience** and so flexibility and tailoring required for reports and dashboards. Expectations will also need to be managed on factors such as level of dynamism; 'Real Time' availability and 'on the go' functionality like other data reports (e.g. those generated from CRM)
  - **Data availability**, accuracy and credibility are likely to be challenging and so it will be interesting to see what the agreed minimum standards will be.
  - **Third Party partners** will need to be aligned on providing information and it is yet to be determined on the consequences of them not being able to provide enough tangible information.
- **Improving operational excellence**, pinpointing issues and identifying areas of optimisation and unrealised opportunities.
- **Scenario planning that is closer to reality** to design recovery, responses and real time controls, testing protocols, early warning systems & trigger alerts and tolerance levels.
- **Validation and due diligence** of 3rd party solution providers.

## 4. Regulators

**Key considerations when responding to regulatory requests that can often be difficult to interpret**

- Regulatory relationships/access will need to be leveraged and where this is not possible the right advisors/consultants will need to be sought. Open to debate whether specific technical expertise will be needed or whether existing regulatory advisors will suffice.
- Need to influence regulators to ensure any reporting obligations and associated templates are realistic. There are limitations for all types and sizes of organisation and so a 'one-size fits all' is unlikely to work.
- Resourcing levels at regulators will have a bearing on responsiveness to queries and items of escalation.
- Multi-jurisdiction operating organisations will need to be prepared for multiple variations as cross-country/regional harmonisation is unlikely. As seen through other regulatory changes, certain regulators will be more onerous than others.'

**"They need to have a willingness to understand what operational resiliency means; what are the expected standards; what has been designed and the ramifications of getting it wrong."**

## Annabelle Plotkin

Armstrong Wolfe Advisor

Former Global Head of Risk, Columbia Threadneedle

Effective assessment, management and governance of Operational Resilience requires our firms to be their best selves: client-focused, process-oriented, thoughtful, integrated, expert, continuously learning and effectively governed.

### Start-up project vs steady state

Whilst there may be a requirement for a 'start-up' project to coordinate and guide the organization to quality Operational Resilience management, ultimately my expectation would be for the business to adopt existing governance paths and ownership (Business Line Operating Cttee, Business Line Risk Cttee, Board Risk Cttee) to ensure that Operational Resilience is understood to be part of the whole business, not just another process which generates new meetings to attend and decks to read.

Using these established structures will also allow the Operational Resilience requirements to be ingrained into the culture of an organization in the way a start-up project would not be able to.

### Key partnerships

Given the need to orchestrate both business requirements and implementation, as well as risk expertise and regulatory requirements, the COO and CRO will need to form as tight a partnership on Operational Resilience as the 3 lines of defence model will allow.

The Compliance team's horizon scanning on regulators' evolving views on Operational Resilience will also be crucial.

## Risk perspective

Our comments in this book have been primarily directed at the 1LOD. I want to note that good management of Operational Resilience also challenges the Risk department to be its best self. Many risk departments have Centres of Excellence which are experts in a particular kind of risk (Cyber, Third Party, Fraud etc), as well as business risk professionals who are experts in each business.

To be effective, both the Centres of Excellence and the business-aligned risk teams need to collaborate to ensure the risk assessment for each business line properly assesses the specific client requirements, vendor profiles and risk vectors in that business. With this approach, each business's resilience plan will be effective for and will resonate with its client and risk profile.

> “The Compliance team’s horizon scanning on regulators’ evolving views on Operational Resilience will also be crucial.”

# Rob Scott

Armstrong Wolfe Advisor

Former Global COO, First Sentier Investors

## While this change is a global regulatory-driven directive, it never made sense to operate the Business Continuity, Crisis Management, Supplier Governance, and Information Security functions in different, disconnected ways.

It makes sense to consolidate these functions within one overall Operations Resilience group, as these are essentially all the Level 1 functions that directly manage the firm's non-financial risks. In saying that, each of the underlying functions spend a different proportion of their time performing resilience-related processes.

Consolidating these functions does not change the 3 Lines of Defence Risk ownership, as the functions are all Line 1 functions that should continue to be managed by Line 1 functional management/leadership, and Lines 2 & 3 should continue to oversee the performance & management of the Line 1 functions.

Implementing an Operational Resilience group, with the functions reporting into that group, only requires 1 head, and potentially 1 other Business Management resource, and could be sourced from the existing underlying functions, without the need to replace internally.

Potential to reduce the number of applications from 1 per underlying function to 1 for the whole Operations Resilience group, to help align the overall Operational Resilience group operating model, to incorporate the additional Regulatory requirements, and potentially reduce the overall system costs. It should be the same operating model globally, applying all national Regulatory requirements across all global offices.

Head of Operations Resilience should report through to the COO, not the Head of Technology, as the consolidated functions are not Technology specific, and support all global functions. In addition, the COO typically has exposure to the overall business positioning & execution strategy, so is better able to incorporate the whole business, and manage the overall business priorities.

One of the 4 functions should be 'Information Security', not just Cyber Security, as all forms of company information should be governed/managed, not just technology-related information.

Establishment of a Financial Services industry Supplier governance utility would improve Supplier governance quality, and reduce costs & complexity, across the industry.

In addition to the COO having overall responsibility, a firm-wide Operational Resilience culture needs to be driven & supported by both the Executive team, and the Board. They need to buy into the need, requirement, benefit to the firm.

The COO & Operational Resilience group needs to agree on what level of resilience is required for the specific firm, i.e. how mature does the resilience need to be for the type of firm, and then educate the Executive team and Board so they are comfortable with the level of maturity the Operational Resilience group is proposing to implement, as it is critical that all parties agree and support the level of maturity, as the maturity level determines both the people and system costs.

The Executive team and Board then need to support the change that's required to implement the agreed consolidated function & operating model, within the required Regulatory timeframe. In order to do this, the Executive team and Board need to understand the benefits of consolidating the functions, and risks of not consolidating the functions, and not implementing the required additional processes to comply with the new regulations.

Compliance needs to work with the Operational Resilience group on what new global regulations the functions need to comply with, and how to best to comply with those regulations.

Risk should already be monitoring the risk associated with the Operational Resilience group. The additional regulations should not impact Risk, apart from the risk of not complying with additional regulations.

The newly created Operations Resilience group need to engage with industry peers, networks, and Consultants to reach a common understanding on how the industry is interpreting each new Regulation, and then decide how the firm will comply, i.e. in the same way, with lighter processes, or with heavier processes.

The Operational Resilience group then needs to monitor how each of the global Regulators respond to their inaugural round of Audits, to confirm whether the Regulator's expectations align with how the firm has decided to comply with each of the Regulators, and make any adjustments where required.

> **"It should be the same operating model globally, applying all national Regulatory requirements across all global offices."**

# So what?

## Nikitas Psyllakis

Armstrong Wolfe Advisor

Former Global Divisional COO, EMEA COO and UK Country Officer
DWS Group

Terms like ‘mundane’ and ‘routine’ are often used to inaccurately portray Operational Resilience as a non-critical, business-as-usual task, underestimating its significance.

Instead, descriptors such as ‘fundamental’ or ‘essential’ better capture its essence as a strategic imperative underpinning an entire operating model. The ‘So What’ of operational resilience becomes evident when considering its overarching purpose: safeguarding a firm’s capacity to deliver critical functions during disruptions, thereby ensuring continuity, maintaining customer confidence, and upholding market stability.

At a time where disruptions are a matter of ‘when’ and not ‘if’, COOs play a pivotal role in equipping organisations to navigate unforeseen events ranging from geopolitical conflicts to cyber threats and health crises, all while safeguarding service integrity. The FCA stipulates that the Chief Operations Function (SMF24) must manage internal operations with robust strategies, ensuring compliance with operational resilience requirements that are comprehensive yet proportionate to the firm’s services.

The consequences of failing to uphold such standards, both in the UK and elsewhere, can result in financial penalties, reputational harm, and, in severe cases, regulatory intervention. A stark reminder of such consequences emerged in late 2022, when UK regulators imposed a £48.65m fine on TSB Bank for operational resilience shortcomings.

COOs also bear the crucial task of advocating for operational resilience at the executive level. They must embed resilience in the organisational culture and decision-making processes, ensuring it receives due consideration in strategic planning and resource allocation. They also have a role to play in effective corporate governance by facilitating transparent communication and accountability, including regular reporting to the board.

Through corporate bodies such as the Operating Committee, COOs need to lead the charge in overseeing the implementation of the operational resilience approach, monitor specific areas of risk and ensure that appropriate measures are in place to mitigate potential threats to the organisation’s operational integrity.

In summary, operational resilience is an ongoing process which is fundamental for the stability and sustainable success of the industry. COOs are uniquely positioned to spearhead the integration of resilience across all levels of operations, extending from the C-Suite to the frontline. By championing this priority, they ensure firms are robust, responsive, and well-prepared to meet unforeseen challenges head-on.

**“Operational resilience is an ongoing process which is fundamental for the stability and sustainable success of the industry.”**

# Armstrong Wolfe Interim

## Bridge the gap, resolve the issue with SME resources

Armstrong Wolfe Interim (AWI) is a global network of former bankers and asset managers available for short to long term contract engagements. Most of this network is Armstrong Wolfe COO and business management alumni and known to the us for many years.

This network is made up of SMEs with successful track records in delivery and execution and reinforced by years spent in regional and global leadership roles. This resource is available on contract for project and programme management, consulting, advisory, and mentoring, within the following areas:

- » Operationalising regulation
- » Structuring and leading remediation
- » 1LoD Controls and Conduct
- » TOM design & implementation
- » Business restructuring
- » Turnaround: distressed projects and programs
- » Running multi-dimensional internal service provisions
- » Cost reviews and programs, design, and execution
- » Product and regional business management

### Our alumni and global network

Those invited to join our network are either transitioning between permanent roles or have committed themselves to a second career in an advisory or consulting capacity. Joining the network is by application, invitation or referral, each applicant is interviewed, and references secured before appointment.

Post successful assessment, full time interims are offered individual iCOOC membership, allowing them to attend selected forums and symposiums, and receive AW articles and periodicals.

Members of the network can be offered an opportunity to be appointed an Armstrong Wolfe Business Advisor, giving them full membership rights in return for supporting the Company's activities, such as participating in forums as a panellist or in the provision of content.

This approach to managing and supporting our network ensures its members remain relevant and up to date on market demands, subjects, and dynamics.

For more information contact **William Parry**
w.parry@armstrongwolfe.com

# Perspectives from the Sell side

**Rob Wilson**

Armstrong Wolfe Advisor

Former BNY Mellon and Merrill Lynch

# Ask a philosopher about your data

Financial institutions are more sophisticated than ever, from the products they provide, the regulatory environments they swim in and the fortitude of their internal infrastructures.

Yet, they remain exposed to uncertainty as much as they allow themselves to be. Operational resiliency not only refers to an organization's ability to operate effectively and maintain critical functions in the face of disruptive events but it also describes a corporate culture where it must be absolutely OK to raise issues. Everything has a time component, which means everything carries a cost.

Operational Resiliency is just as much about the people who run an organization as it is about the data identified by that organization. You need to be able to ask questions about the level of your resilience before you undergo difficult days so that you have internal routines to address the findings.

Further to this, organizations must demonstrate to regulators they have the frameworks to proactively manage themselves. Using the right approaches, these frameworks will create connectivity inside an organization where the client, the firm, and the regulatory lenses are used to organize conversations so that people, platforms and priorities are understood by everyone.

This mindset is nothing new. Let's refer to the philosopher Aristotle who wrote at length about risk as the ancient Greeks sought to build and codify their society into early attempts at civilization.

Aristotle marvelled at how the human condition is characterized by chance, probability, uncertainty, and unpredictability. He recognized our survival depended on abilities such as practical wisdom and capable decision making.

## What does all this mean?

In order to make progress in operational resiliency, it is essential to make a commitment to outlining the understanding of best practices, or establish where you have gaps. Above all, Aristotle highlights the virtue of good judgement which requires considering potential risks and avoiding unnecessary danger.

Good judgement encompasses combinations of principles and assumptions which allow organizations to prepare for external disruptions and minimize the impact as best as the situation allows.

These principals also examine the internal uncertainties which often accompany these types of events. A starting principle might be that all activities have a financial impact, either in terms of pro-actively putting in solutions or via a post-mortem where an event has led to an unexpected financial outcome.

A starting assumption will show that there is an appreciation that reviewing the firm's capabilities to become more robust and less brittle over time.

A strong COO group can lead these key discussions by identifying the persons who can engage on the important topics with operational resiliency across the differing business lines and, at the same time be inter-operable across the various lines of defence.

# Richard Austin

Armstrong Wolfe Advisor

Former Global COO Technology and Innovation, Standard Chartered

Operational Resilience has an ever increasing level of importance in keeping the financial services industry safe and secure. Both regulations and industry responses continue to evolve but there is a key role to play for all 3LoDs and COOs to meet the requirements.

**Who is responsible for Operational Resilience?**

> **RA** - *Ultimately the Board and the C-suite are responsible but all parts of the organisation across the 3LoDs need to engage. Some key aspects are the responsibility of Technology but definitely not all.*
>
> *Therefore, Group Op Res responsibility frequently rolls up under the COO in order to govern and execute across organisational silos. On the Tech side, 'system' resilience is usually addressed by the Group CIO and the Head of Infra (CTO) given their responsibility for service management.*

**Why does its importance continue to be elevated?**

> **RA** - *Banks are increasingly complex and interconnected organisations both internally and externally. Technology advancement and adoption across the industry necessitates ever rising service levels and resilience.*
>
> *Customer expectations are less and less tolerant of outages and operational service interruptions. Regulatory focus has increased scrutiny and Op Res provides the umbrella for relevant Non Financial Risk Types (notably Op Risk, Tech Risk, Cyber, BCP / DR, 3rd Party and to a lesser extent Data).*

**Does it require a different approach to managing risk?**

> **RA** - *Many of the risks identified are not new and should be managed under the existing Enterprise Risk Management Framework with resilience requirements addressed within each of the Risk Types tagged to Op Res.*
>
> *However, it's the 'basket weave' across journeys, people, process and technology that is key and a holistic approach is required to address risk. It is most certainly not just a technology or operations problem and notably has elevated third party risk to a higher level than previously governed, reflecting the financial ecosystems we operate in and use of common industry platforms e.g. Public Cloud, payment services etc.*
>
> **RA** - *The consensus approach to address Op Res as articulated by a few of the consultancies seems to be:*
>
> 1. *Identify critical journeys, processes, operations and functions*
> 2. *Assess risks and set tolerances in terms of business impact*
> 3. *Map interconnections and pay careful attention to third parties (and even fourth parties!)*
> 4. *Verify and test the resilience solutions, refine and enhance.*

### How does it impact the 3LoDs?

**RA** - *All are involved but fundamentally the risks need to be mitigated by the actions of the 1LoD vs the requirements of the Regulators interpreted by the 2LoD and audited by the 3LoD.*

*It continues to reinforce the need to have a very effective 1LoD Risk and Governance capability (including Chief Control Officers, CCOs) aligned to the COOs that interact across silos and can respond to the complexity required for Op Res (plus emerging risks in general). It also needs a lighter, nimbler 2LoD to help the organisation prioritise appropriately and to risk accept vs impact tolerances as these have to be judicious.*

### Are there geographic differences e.g. for Asia?

**RA** - *Although the UK, Europe and the US have led the way, local regulators notably HKMA and MAS have gone through a consultative process and are broadly in line so far with the global regulators.*

*However, DORA in Europe is the interesting one for me as it has picked out specific third party offerings (such as Data Centres or Cloud) for Regulatory attention. Given their importance it makes sense but it also raises questions for emerging technology too e.g. does AI now need to be specifically risk managed? Is Nvidia already too big / important to fail and therefore users including Banks need to factor that in to their Operational Resilience approach?*

## Katy Matvey

Armstrong Wolfe Advisor

Former APAC COO, Wells Fargo

# Overview and APAC regulatory focus

Operational resilience is an evolution from already existing risks and requirements around business continuity, third party reliance, process robustness.

**As the risks in these areas have increased due to cyber threats, increased reliance on outsourced technology (including cloud) and more global interconnected processes, there is now a heightened focus on Firms' preparation for resilience to address these risks.**

In APAC, this has been a focus of both the MAS and HKMA as well as JFSA and APRA. The MAS and HKMA require licensed institutions to conduct self-assessments and prepare an action plan to address any weaknesses.

In addition, certain aspects of resiliency, such as third part risk management, have been a high focus of the MAS and other regulators in the region.

The regulators are now expecting a higher level of focus on operational resiliency in order to protect consumers but also the financial system.

## New Risk Type?

At the core, I don't believe this new term or focus is different from fundamental risk management and expectations that have already been in place. The expectation is that the firm should understand its products and processes and the risks that those generate, including external risks such as cyber-attacks or natural disasters.

Therefore, the focus should continue to be on the identification of critical processes, understanding the risks, setting an acceptable risk tolerance, creating controls and then monitoring/testing of those controls. This would include scenario or stress testing as expected by regulators.

The **'wrapper'** term is interesting and can be helpful to bring the various operational resiliency topics together to be reviewed more holistically. However, many of those topics/ risks have aspects other than resiliency.

For example, third party risk has other risks involved beyond those related to resiliency. Therefore, in some ways resiliency is like a horizontal slice across many topics but it doesn't encompass everything about those topics/risks.

> **"At the core, I don't believe this new term or focus is different from fundamental risk management and expectations that have already been in place."**

## Governance

Because I don't see this as a specific new risk type, I see the responsibility with the front line as part of understanding and managing their risk. Business leaders need to understand the risks in their processes, systems, vendors and how that risk is being managed.

They will need to rely on various partners to supply information on risks/controls for different aspects, including technology vendor management, cyber security.

That is where I see the horizonal slice or wrapper being useful – to pivot the information to look at it specifically from an operational resilience lens but not to remove it from fundamental risk reviews.

COOs are probably best placed to have all the information across the topics. They are often responsible for Operations, Third Party/Vendor management, Property and Security and either manage Technology directly or have a close partnership.

They are also often responsible for the RCSA process, which gives insight into the critical business processes and risks. The APAC regulators have not been prescriptive about how or who should manage the risk or be responsible for collation and reporting on this topic. It is interesting that the UK has put this regulatory demand of the SMF 24.

Essentially the regulator has put it as responsibility of the tech leader but in many organizations that leader is not responsible for other aspects of resiliency. This seems to potentially narrow the focus to just be tech aspects of resiliency versus the full spectrum of risks related to resiliency.

> **"The 'wrapper' term is interesting and can be helpful to bring the various operational resiliency topics together to be reviewed more holistically."**

# George Nunn

Armstrong Wolfe Advisor

Former COO Global Markets and Global Banking Americas, BNP Paribas

## To help enliven the discussion on Operational Resiliency, here are my thoughts on a few areas for investigation.

Non-Financial Risk Management entails a comprehensive mapping of potential risks, controls, and the likelihood of disruptions spanning Technology, Operations, Cybersecurity, and people processes.

Non-Financial Risk Management is essentially a systematic inquiry into what could go wrong. Operational Resiliency, on the other hand, focuses on fortifying your organization against these potential disruptions. It involves strategizing to minimize business interruptions by considering the tolerance levels for losing a business line, whether for a day, a week, or even a month, while evaluating the impact on revenue, customer experience, and reputation.

Similar to the analysis conducted in Enterprise Risk Management, Operational Resiliency places the responsibility for risk exposure, financial losses, market disruption, and other impacts squarely within the purview of the first line of defence (1LOD). The tone for addressing Operational Resiliency must be set at the 1LOD level, mandating the involvement and attention of all functional support teams thereafter.

## Resilience is insurance

It costs money but pays off handsomely during crises. Over time, it can even evolve into a competitive advantage. For instance, companies utilizing multiple cloud providers not only bolster their resilience but also gain cost advantages by directing workloads to the most cost-effective provider at any given time.

Achieving resilience necessitates a fundamental overhaul of various business processes, including technology, operations people, and strategic planning processes. This shift mirrors the evolution seen in technology development teams - from Dev to DevOps to DevSecOps - where considerations of production and cybersecurity are seamlessly integrated into the IT development chain.

IT development teams will need to progress to DevSecOps+OpRes, with a concerted effort to embed Operational Resiliency into production operations, vendor selection processes, and strategic planning.

In designing business workflows, first-line teams will need to evolve to build-in redundancy at inception, mimicking the strategy, long employed in data centre management: maintaining primary and backup data centres, dual electricity providers, and multiple real-time financial data sources. Extending this redundancy to pre-trade, execution, and post-trade systems and workflows across both front and back offices is crucial.

On the face of it this looks like a dramatic cost increase - adding vendors as a backup is costly, and in the case of some industry utilities not possible. The industry may need to rethink vendor relationships - with two vendors selected for eligible services and fees linked to volumes processed to systematically ensure resiliency while mitigating overall cost.

**Second line teams would focus on testing for gaps in design and reliability of the chosen vendors.**

To further support the industry in navigating unforeseen challenges, Armstrong Wolfe could host a Symposium on lessons gleaned from the Ukraine war. This conflict offers invaluable insights into preparation, innovation, rapid adaptability and the integration of real-time data into strategic decision-making.

These lessons are not only relevant to military and societal resilience but also hold significant implications for business leaders, particularly in sectors like banking, where adaptability and resilience are paramount strategic imperatives.

# Penny Cagan

Armstrong Wolfe Advisor

Former Americas Head of Operational Risk, UBS

I consider the discipline of Operational Risk to be about resiliency at its core. If some in the industry consider Operational Risk to be solely about avoiding losses, they might miss how important Operational Risk frameworks, practices, and tools are to bolstering organizational resilience.

The concept of Operational Resilience, however, can be a convenient wrapper and assist with a call to action to get management attention and support. At the end of the day, Operational Risk and Operational Resilience are so interconnected that they must be managed together.

The good news is that many financial institutions have mature or maturing Operational Risk frameworks, practices, and tools in place for managing resilience, while non-financial institutions (many of which provide 3rd party services to financial institutions) are increasingly putting Operational Risk Management programs in place.

These frameworks, practices, and tools allow organizations to respond to and learn from disruptions and to be able to deliver and execute critical processes and respond to client needs with minimal disruption.

Operational Risks that result from events where resiliency is critical to a firm's ability to recover and protect its reputation are often interconnected. This includes cyber, technology, 3rd party, supply chain, and increasingly, geopolitical risks. There is also growing exposure to concentration risk, with limited suppliers who provide critical services such as those related to the Cloud.

Existing Operational Risk frameworks, practices and tools are designed to look across these risks if they are used intelligently and comprehensively and are more than annual check-the-box exercises.

Central to managing a firm's resiliency is the creation of a library of Operational Risk Scenarios that identify severe but plausible risks. These scenarios can be powerful tools in the understanding of events with high impact and inform resiliency desk-top exercises and walk-throughs. They are most effective when they are multi-dimensional and consider exposure associated with the convergence of multiple risk types.

Risk and Control Self Assessments (RCSA) are also valuable tools in the management of a firm's resiliency efforts. They provide insight into a firm's current and emerging risks, and control environment. A strong practice is to stress the controls identified through the RCSA process -- i.e., walk through events that could occur if the identified controls do not operate effectively if at all – and use the results to further inform Scenarios.

The creation of end-to-end views of a firm's Operational Risk exposure is central to the understanding of its ability to be resilient in the face of an event that might strain its ability to operate. This includes the identification of the firm's most critical processes and ongoing assessment of associated risks and controls.

“Resilience is not just a framework and process issue, as it is also a people issue.”

It is also equally critical to have a reporting program in place that provides transparency on current and emerging risks and controls to business management and the executives and board at the top of the house. It takes a certain skill and expertise to be able to articulate both broadly and deeply what those end-to-end risks and controls are.

Finally, resilience is not just a framework and process issue, as it is also a people issue. The partnership between the various disciplines – the first line Control Officers that report through the COO, the second line Operational Risk Managers, the specialists in technology and business continuity areas – is critical to a strong resilience program.

This takes people who are highly collaborative, able to work across disciplines and support each other in the management of risk.

Like most risk disciplines, it comes down to the firm’s risk culture and ownership of risk across all the lines of defence and disciplines. It requires both specialists who understand specific disciplines like cyber and technology deeply and generalists who can assess and articulate a firm’s end-to-end risk profile.

It also requires leaders who are committed to creating learning organizations, so that lessons can be learned from the more routine events and control issues remediated as they occur.

Ultimately, the better an organization is at managing Operational Risk, with the right people, frameworks, practices, and tools in place, the more resilient it becomes over time and the more it can manage through disruptions in this ever-more complicated environment that we all work in.

# Randi Abernethy

Armstrong Wolfe Advisor

Former Banking and Capital Markets Specialist Leader, Deloitte

It's a topic I have definitely been in and around given my experience as a current Enterprise Risk Officer.

While Enterprise Risk and Operational Resilience frameworks and perspectives are different, there's a lot of overlap. From my perspective, establishing robust ERM and Ops Resilience plans and frameworks is not only a 'must have' but they work together and complement each other very well. Both include identification of cross organizational risks with associated mitigating controls, along with plans to respond to risks both reactively and proactively to ensure resilience. I like the concept of the 'wrapper' that has been set out in the PoV already, and do agree with that. A few thoughts from my perspective as to what is critical to strengthen that wrapper:

## Culture

Setting the right operational resilience and general risk management culture is critical to achieving a cohesive approach and perspective with regards to resilience, risk and controls. Incorporating this perspective into an organization's strategy and support of its mission and objectives is key in promoting and maintaining that culture across the organization.

## Interconnectedness

The financial services community is highly interconnected through vendors, customers, counterparties, etc. Operational resilience planning therefore shouldn't happen in a vacuum. It should be approached collaboratively both across industry and with regulators.

## Communication

Tying both the previous points together is communication. Communication is key within an organization, across organizations and with regulators and industry bodies to ensure collaboration, awareness of best practices and awareness of any incident that could impact a wider ecosystem or become systemic.

> **"Setting the right operational resilience and general risk management culture is critical to achieving a cohesive approach."**

# The COO Debating Society

## Since 2015 Armstrong Wolfe has been running round table debates supporting the Chief Operating Officers of Markets, Banking and Asset Management.

Additionally in 2016 Women in the COO Community (WCOOC) was established and in 2020 the International COO Community (iCOOC). 2023 saw a re-purposing of WCOOC, repositioning it to play an on going and important role as part of Ad Centrum, the COO Centre of DEI Debate. A world where everyone belongs.

Introduced at Armstrong Wolfe's inaugural COO Summit in February 2023, the COO Debating Society held its first debate, Purpose vs Controls as the single means to manage conduct.

Through debate the society seeks to draw attention to subjects at the heart of the COO's mandate. The judges and audience are briefed they can only vote on the strength of the argument presented, not any predetermined views on the subject.

The debates will often place aspects which are complementary against each other, where both are clearly needed for success but you can only vote for one.

The debate affords each team the opportunity to take the audience on a two dimensional journey to a result that is not predetermined, as both are often needed but the strength of the argument defines the result. The debate is used to break down and present the strengths of each in its own right, and prompt thought on important aspects of the COO's day to day activities.

The COO Debating Society is open to the directorate of corporate members of iCOOC and Ad Centrum, the Society's alumni (previous judges, debaters and hosts), and invited guests.

# Thoughts on Conduct & Control

**Toby Billington**

Armstrong Wolfe Advisor Controls and Conduct

Former Citi

**Ed Clementi**

Armstrong Wolfe Advisor Controls and Conduct

Founder & CEO, Inspired Fire

# The Importance of a Strong Culture for Effective Operational Resilience

In the banking industry, operational resilience is defined as ‘the ability of banks to withstand, adapt to, and recover from disruptions that affect their operations, ensuring they are able to continue to provide critical services to their clients and customers and to report accurate data to their regulators.’

In an era marked by technological advancements, regulatory changes, and evolving customer expectations, maintaining operational resilience has become paramount. A key, yet often under appreciated, factor contributing to this resilience is the organizational culture. This article delves into why culture is vital for operational resilience in the banking industry, exploring its impact on risk management, regulatory compliance, customer trust, innovation, and crisis management.

## The Power of Leadership and the Tone at the Top

Imagine a ship navigating through a stormy sea. The captain's demeanour, decisions, and values set the tone for the entire crew. This is what leadership tone at the top represents—the ethical climate and organizational culture established by senior management.

It's the embodiment of the values, beliefs, and behaviours that leaders expect from themselves and their teams. When the tone at the top is strong, it permeates every level of the organization, influencing decision-making, employee behaviour, and overall resilience.

Creating a sustainable culture of excellence is essential for any organization aiming for long-term success and growth. Yet, many leaders struggle to invest deeply in this vital area. Short-term focus, resource constraints, and resistance to change often stand as significant hurdles.

However, a strong leadership tone ensures that the organization lives by its stated values and culture, fostering trust, accountability, and a sense of purpose among employees. When leaders consistently model the values they espouse, it reinforces the importance of those values and encourages employees to adhere to them, even in times of crisis.

## The Role of Culture in Risk Management

Risk management is a cornerstone of operational resilience. Banks face various risks, including financial, operational, cybersecurity, and reputational risks. A robust risk management culture ensures that all employees, from top executives to front-line staff, understand and care about the importance of identifying, assessing, and mitigating risks.

**1. Risk Awareness and Reporting:**

A culture that promotes risk awareness encourages employees to report potential issues without fear of retribution. This openness leads to early identification and mitigation of risks. Senior management plays a critical role in ensuring that employees have the psychological safety to report without fear. Sadly, this is all too often a promise that is not upheld, and once this trust is broken, reporting dries up completely.

**2. Accountability and Responsibility:**

When a culture of accountability is embedded, employees take ownership of their roles in risk management. This sense of responsibility ensures that everyone is vigilant and proactive. Managers and leaders set the tone by demonstrating their commitment to risk management, which cascades throughout the organization.

**3. Training and Continuous Learning:**

A culture that prioritises continuous learning and training helps employees stay updated on the latest risk management practices and regulatory requirements. Regular, relevant training sessions, workshops, and seminars help to ensure preparedness and competence for when something does go wrong, enhancing the bank's overall resilience. Conversely, mindless, online, irrelevant, and repetitive training has the exact opposite effect.

## Enhancing Regulatory Compliance

Regulatory compliance is critical for the banking industry, given the stringent regulations designed to protect consumers and maintain financial stability. A strong compliance culture ensures that the bank adheres to these regulations consistently and effectively.

**1. Ethical Behaviour and Integrity:**

A culture that values ethics and integrity supports compliance by encouraging employees to adhere to laws and regulations not just because they are required to, but because it is the right thing to do. This intrinsic motivation leads to more consistent and genuine compliance efforts. The integrity and sincerity of senior managers' communication is vital to this effort. Nothing undermines an ethical culture faster than an insincere leader speaking cultural platitudes which staff know they don’t really believe.

**2. Proactive Compliance Management:**

Banks with a proactive compliance culture anticipate regulatory changes and prepare in advance. This forward-thinking approach allows them to adapt quickly to new regulations, minimizing disruptions and maintaining operational continuity.

## Building Customer Trust and Confidence

Customer trust is a foundational element of the banking industry. Operational disruptions can erode this trust, making resilience critical. A culture that prioritises customer-centricity can enhance operational resilience by fostering trust and loyalty.

**1. Customer-Centric Values:**

When a bank's culture is centred around customer needs and values, it prioritises maintaining service continuity even during disruptions. This focus on customer satisfaction drives efforts to develop robust contingency plans and resilient systems.

**2. Transparent Communication During Crises:**

In times of disruption, transparent and timely communication with customers is crucial. A culture that values openness ensures that customers are informed about issues and the steps being taken to resolve them. This transparency helps maintain customer confidence and trust. As above, the sincerity and integrity of these communications are of paramount importance. Don't be quick and transparent if you are not being honest.

**3. Consistency and Reliability:**

A culture that emphasizes reliability ensures that customers experience consistent service levels. Even in the face of disruptions, banks that prioritise operational reliability can uphold their service commitments, reinforcing customer trust.

## Fostering Innovation and Adaptability

The banking industry is undergoing rapid transformation driven by technological advancements and changing customer expectations. A culture that encourages innovation and adaptability can significantly enhance operational resilience. Sadly, this is a factor that is in short supply in mainstream banking. Most interestingly, although we give some pointers below as to how innovation and agility can reduce operational risk, it is often operational resilience that is used as a reason for not innovating and continuing to do things the same way.

**1. Embracing Technological Advancements:**

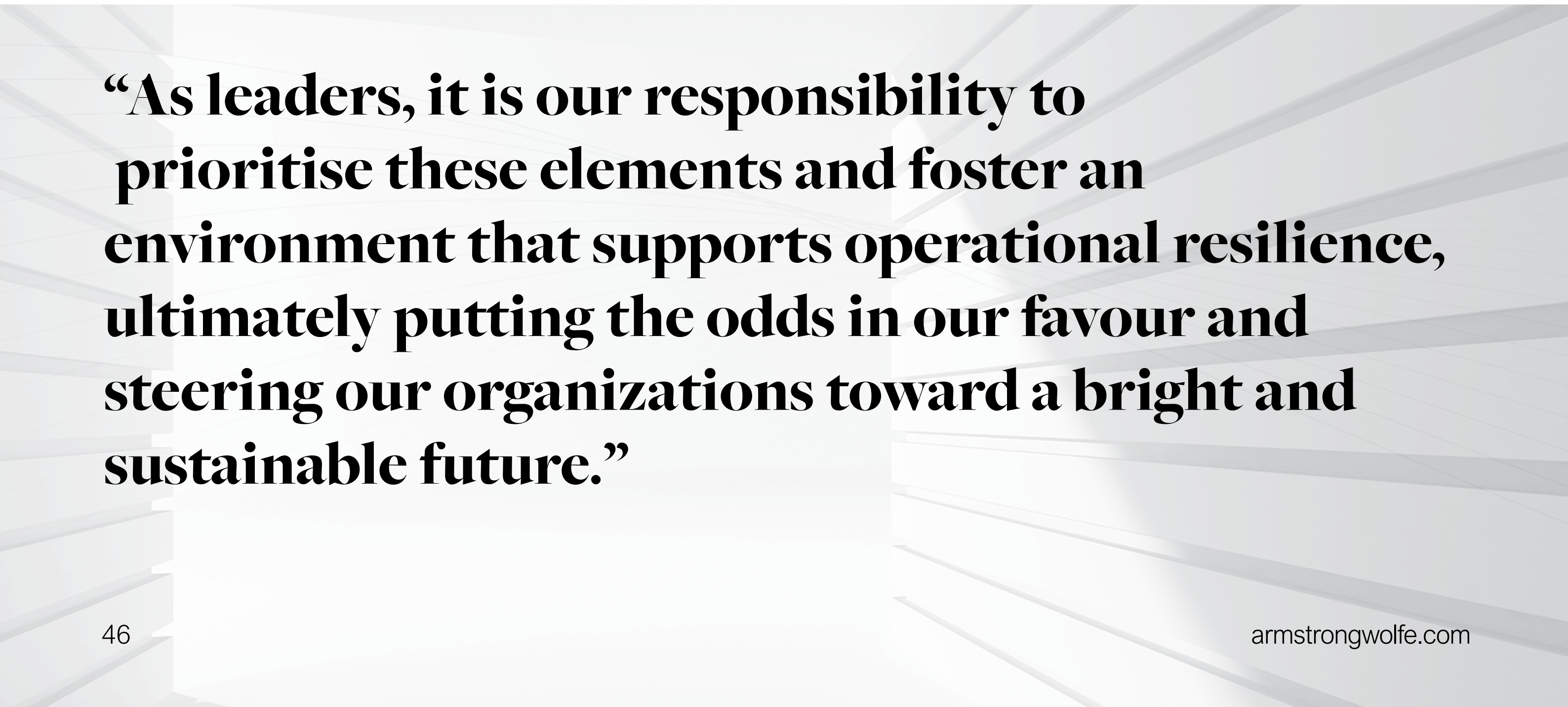
A forward-thinking culture that embraces new technologies can improve operational resilience by streamlining processes, enhancing security, and enabling faster response to disruptions. For example, adopting artificial intelligence for fraud detection has helped banks identify and mitigate risks more effectively and much faster.

**2. Agility and Flexibility:**

An agile culture enables banks to adapt quickly to changes and unexpected challenges. This flexibility is crucial for maintaining operational continuity during disruptions. Teams that are accustomed to iterative processes and continuous improvement are better equipped to handle unforeseen events.

**3. Encouraging Experimentation:**

A culture that encourages experimentation and tolerates failure fosters innovation. By allowing employees to test new ideas and approaches, banks can develop more resilient systems and processes. This innovative mindset is essential for evolving in a dynamic environment and is not one that is a natural fit with current, mainstream banking practice.



> **"As leaders, it is our responsibility to prioritise these elements and foster an environment that supports operational resilience, ultimately putting the odds in our favour and steering our organizations toward a bright and sustainable future."**

## Effective Crisis Management

Effective crisis management is a critical aspect of operational resilience. The way a bank responds to and recovers from a crisis can significantly impact its long-term stability and reputation. A strong organizational culture plays a pivotal role in effective crisis management.

**1. Preparedness and Planning:**

A culture that prioritises preparedness ensures that comprehensive crisis management plans are in place. Regular, realistic, and relevant drills and simulations help employees understand their roles and responsibilities during a crisis, enhancing the bank's ability to respond effectively.

**2. Leadership and Decision-Making:**

Strong leadership is crucial during a crisis. A culture that empowers leaders at all levels in the bank to make swift, informed decisions can significantly improve crisis response. Empowering lower-level managers to make quick decisions in areas where they have relevant expertise is vital. Getting everything signed off at senior level or committee creates bottlenecks and delays. Leaders who can demonstrate calmness, decisiveness, and empathy will best guide the organization most effectively.

**3. Collaboration and Teamwork:**

A collaborative culture fosters teamwork and coordination, which are essential during a crisis. When employees across departments work together seamlessly, they can address issues more efficiently and restore normal operations faster.

## The Synergy of Control and Culture

Imagine the ship again, this time with a crew that not only trusts and supports each other but also follows well-established protocols to handle emergencies. This synergy between culture and control is what creates operational resilience. Robust controls within a well-established healthy culture naturally increase an organization's resilience. This balance is crucial for long-term sustainability.

While controls provide the necessary structure and safeguards, culture ensures that employees are engaged, motivated, and aligned with the organization's goals. In a well-balanced organization, employees understand the importance of compliance and risk management because it is ingrained in the culture. They do not view controls as bureaucratic hurdles but as essential components of their daily responsibilities. This cultural alignment makes it easier to implement and maintain effective controls, as employees are more likely to invest in quality and adhere to policies and procedures when they see their value.

## Conclusion

Operational resilience is the key to thriving in an unpredictable business environment. The leadership tone at the top plays a pivotal role in establishing and maintaining a resilient organizational culture and robust control mechanisms. By living their values and setting clear expectations, leaders can create an environment where employees are motivated to act in the organization's best interests and are equipped to handle disruptions effectively.

Creating a sustainable culture of excellence, overcoming short-term focus, resource constraints, and resistance to change, and ensuring robust controls are not just strategic choices but essential actions for safeguarding the future of our organizations.

inspired fire®

Make an Impact. Feel an Impact.

# Ignite Your Leadership Legacy. Lead with Confidence and Purpose. Foster a Culture of Pride.

Great leadership is the foundation of exceptional cultures; it begins and ends with those who lead. At Inspired Fire, we are committed to transforming the leadership landscape by championing authenticity, empathy, and inspiration. This form of leadership empowers individuals to excel, fosters innovation, and ensures lasting success. Anything less falls short of the immense responsibility that comes with being a leader.

At Inspired Fire, LLC, we empower leaders to ignite their leadership legacy and drive transformative change. Our mission is to cultivate leaders who embody empathy, authenticity, and inspiration, fostering resilient and sustainable cultures that achieve unparalleled success.

Are you proud of your organization's culture?
Are you leading with purpose and confidence?
What is your legacy?

Building a great culture takes intention, time and commitment, but the impact is profound and enduring. Join Inspired Fire, and let's shape a legacy of leadership that inspires and transforms.

Contact us today to start your journey towards exceptional leadership and a thriving organizational culture.

Ed Clementi, Founder & CEO of Inspired Fire, LLC
www.inspiredfire.net

**Fahreen Kurji**

Chief Customer Intelligence Officer

Behavox

# Managing Operational Risks with Advanced AI: Insights from Behavox

In today's financial landscape, operational risks are a persistent challenge, threatening the stability, reputation, and legal standing of organisations.

These risks, ranging from insider threats to market abuse, demand robust solutions. Financial firms face critical questions such as:

1. How can we effectively identify and mitigate operational risks?
2. How do we ensure compliance with ever-evolving regulatory expectations?
3. What role can advanced technology, like AI, play in enhancing our risk management frameworks?
4. How do we maintain a secure and resilient operational environment amid growing threats?

Addressing these risks requires robust solutions and advanced technology. In this interview, Behavox, a leader in AI-driven risk management, shares how their innovative tools tackle these issues head-on.

> **Interviewer:** *How can financial firms effectively identify and mitigate operational risks?*

**Behavox:** Operational risks in financial services often stem from failures in internal processes, people, and systems, or external events. Two significant risks are insider threats and market abuse. Insider threats involve employees misusing their access to confidential information, potentially causing severe financial and reputational damage.

Market abuse includes actions like market manipulation and insider trading, which undermine market integrity and investor trust. For example, the SEC has imposed significant fines on firms failing to detect insider trading, such as the $16 million fine on Nomura Securities in 2020.

We address these challenges with a suite of AI-powered products. Our communication surveillance platform, Quantum, monitors and analyzes employee communications to detect unethical behaviors and market abuse using advanced machine learning algorithms. This proactive approach allows firms to address issues before they escalate, ensuring higher levels of compliance and risk management.

> **Interviewer:** *How do firms ensure compliance with ever-evolving regulatory expectations?*

**Behavox:** Ensuring compliance with regulatory expectations is critical. Regulatory bodies like the SEC and FINRA mandate the archiving of communications as a regulatory necessity. Quantum is pivotal in monitoring and analyzing employee communications for unethical behavior.

Our Intelligent Archive goes beyond mere storage by enhancing compliance with advanced search capabilities, allowing swift responses to regulatory inquiries. Falcon, our human risk management platform, predicts and manages human behaviors that could escalate into risks.

Additionally, our Pathfinder chatbot provides AI-driven guidance for finance professionals, helping them navigate complex compliance queries and prevent inadvertent breaches.

> **Interviewer:** *What role can advanced technology, like AI, play in enhancing risk management frameworks?*

**Behavox:** AI is at the core of our solutions, significantly enhancing our risk management frameworks. Falcon analyzes behavioral patterns to predict and manage risky actions, allowing early intervention.

Our specialized large language model for the financial sector, Behavox LLM 2.0, offers precise explanations, summarizations, and complex financial calculations, enhancing the overall risk management framework. AI's ability to process vast amounts of data quickly and accurately makes it indispensable for identifying potential risks and ensuring compliance.

> *Interviewer: How do we maintain a secure and resilient operational environment amid growing threats?*

**Behavox:** Transparency and security are essential for maintaining a resilient operational environment. Our AI models are designed to be explainable, providing clear insights into their decision-making processes. This transparency is crucial for internal teams and regulators to trust and verify the outcomes driven by our AI. We support over 46 languages, ensuring our solutions can serve organizations worldwide.

This multilingual capability overcomes geographical and linguistic barriers, maintaining a unified standard of compliance and risk management across global operations.

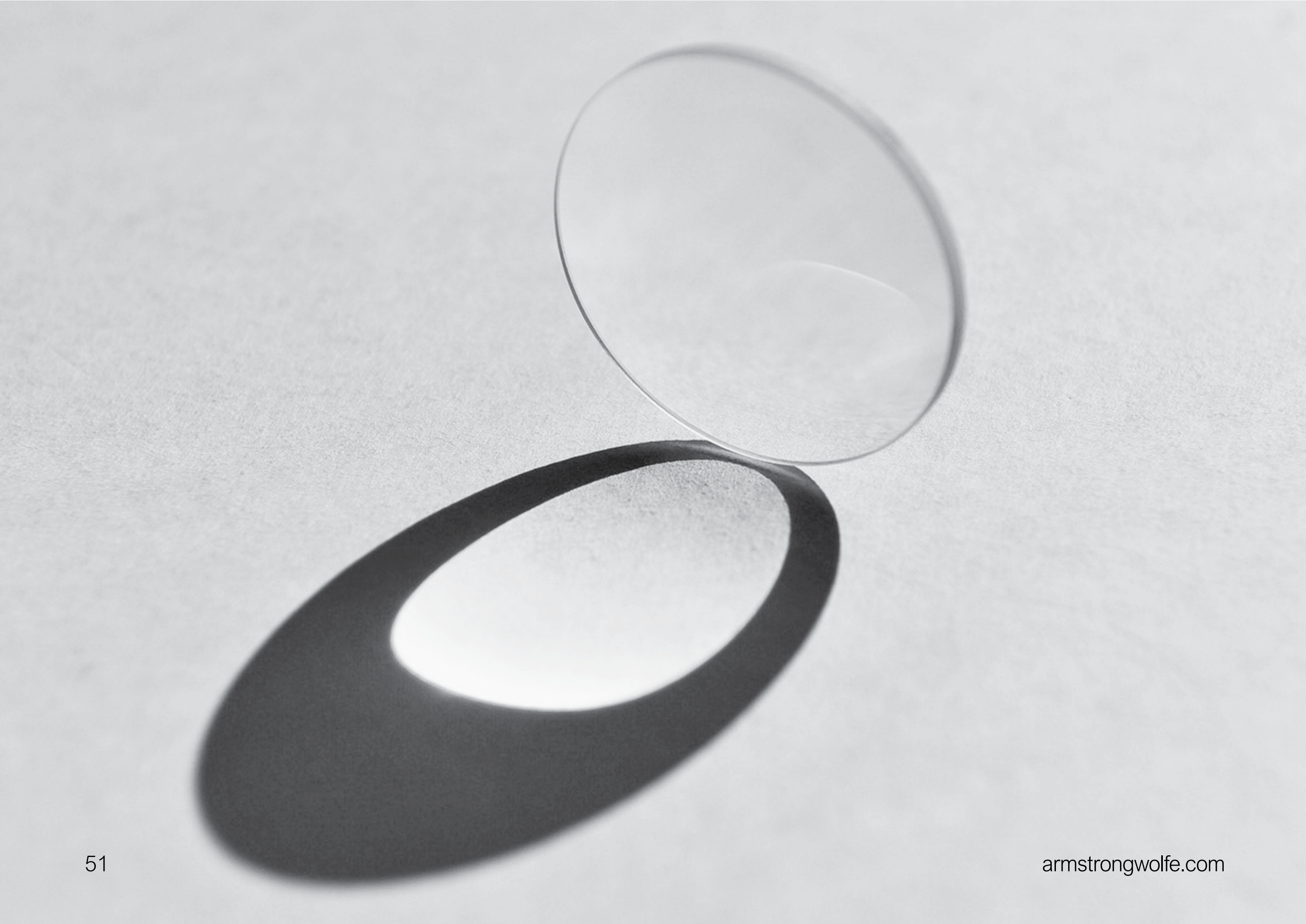
Our commitment to security is demonstrated through rigorous standards, including SOC II certification. We ensure that all data is handled in a secure, compliant, single-tenant environment, providing peace of mind about the integrity and confidentiality of their data.

Real-world examples, such as the stringent data protection requirements in the EU's GDPR, underscore the necessity for such robust security measures.

Behavox's advanced AI solutions empower financial firms to navigate complexities with confidence, ensuring a safer and more efficient operational environment. By proactively addressing operational risks, maintaining compliance with regulatory expectations, leveraging advanced technology, and ensuring security and transparency, Behavox helps businesses protect their integrity and enhance productivity.

“Ensuring compliance with regulatory expectations is critical.”

# Looking Through a Regulatory Lens



# Georgina Philippou

Armstrong Wolfe Advisor

Former FCA COO and FCA Senior Adviser Equality

While operational resilience tends to focus on IT and cyber resilience, the pandemic has shown us that it is in fact about all aspects of a firm's operations, including the flexibility and resilience of the built environment and the flexibility and resilience of staff at all levels.

The Post Office scandal has proved, if it needed proving, that outsourcing to a third party supplier is not a get out jail free card. DEI also plays an important role here – an organisation that has embraced DEI, in particular the cognitive diversity that should flow from DEI, is more likely to be operationally resilient.

A firm which has a safe to speak up culture is more likely to be able to work across silos to manage operational risk. A firm which ensures that it has diverse suppliers and that those suppliers share its cultural values around DEI and psychological safety is more likely to be operationally resilient.

The COO's role is critical, not just because they hold the SMF for operational resilience but because they can advocate for operational resilience in its widest sense at all levels of the organisation, they can act as the bridge between the first, second and third lines of defence, and they can challenge those areas of the business where profit and market share may conflict with resilience.

Where COOs are responsible for IT and/or cyber, they can manage the tensions which sometimes exist between the two functions. Essentially, a good COO can bring the organisation together and keep operational resilience front of mind. The COO is also an important link to the CEO, and the Executive generally, and the Board, ensuring that they have sufficient understanding of the issues to enable them to provide effective support and challenge.

So when the FCA examines operational resilience it may focus on IT and cyber but it may also take a more holistic approach, considering operational resilience as an indicator of or reflection of a firm's culture and governance. It may focus on the COO/SMF 24 who is responsible for operational resilience, but it will also hold the wider executive and the board to account. It will look at operational resilience as an ongoing cycle of horizon scanning, forecasting, preventing, responding to and recovering from incidents and crises.

The FCA will also take an outcomes focussed approach, looking at operational resilience not just as a matter of keeping an individual firm going, but at the impact operational issues in a single firm can have on customers and across a market. The FCA will expect a firm to have a clear narrative behind the approach it is taking to operational resilience, reflecting the fact that there is no one size fits all approach.

Where the FCA finds operational resilience weaknesses, it has a range of options when it comes to action, depending on the severity of the issues and the impact on market confidence and consumer protection. These options range from supervisory action, s166 reports, regulatory guidance, Dear CEO letters, multifirm work, through to enforcement action against firms and individuals, including financial penalties and prohibitions.

**"The FCA will expect a firm to have a clear narrative behind the approach it is taking to operational resilience."**

# Ted MacDonald

Armstrong Wolfe Advisor
Senior Technical Specialist
Financial Markets Standards Board (FMSB)

This COO Perspectives report pulls together a great deal of information, insights and some points for debate. Key areas of non-financial risk commented on include operational, cyber, 3rd party vendors, technology platforms and business continuity.

It is also important to step back and consider the downside risk of operational resilience from a human risk perspective. The entire discussion could be split into two streams: Infrastructure Risk and Human Risk with the point being to raise the profile of the latter.

It is often the case that breaches or failures, in what would typically be reported as technical matters, have their roots in basic human risks like staffing levels, specialist expertise or experience, inappropriate delegation, inadequate training or deficiencies of another kind that result in the sudden failure of a system, a missed process step, a bad judgement call or just a wide-ranging inability to cope with operational stress.

Catastrophic events, for example, a hurricane get attention but operational stress often manifests in lesser forms like high winds that nevertheless can result in a disruptive outage. The resilience risk shifts to how well people communicate and work together towards a common purpose, goal or outcome.

Positive results may rely on the exercise of good judgement but this is hard to develop in an environment where the strict emphasis on following the rules undermines the skill of navigating grey areas.

Resilience metrics tend to focus strongly on capacity levels, tolerances, breach trends and other backward looking safety measures.

Creation of some new, additional metrics that focus on key behaviours and the wider health of the organisation were recently identified by FMSB members in its Conduct and Culture MI report as a key area for development.

The challenges of managing a complex organisation reminds me of a giant mosaic. All the pieces must be stitched together and each unit or team may have its moment in a given circumstance; none are superfluous. The key skill is navigating among the many silos.

The overall risk management framework, developed by the organisation as a whole, should be the key reference point in how and where things are done. The FMSB's report states that the 3 Lines Model serves only to assess the design effectiveness of the risk management framework, nothing more.

**“My message is just a timely reminder that all of our policies, processes and infrastructure are in partnership with humans.”**

# David Blunt

Armstrong Wolfe Advisor

Former Head of Conduct Specialists, Supervision FCA

## From a regulatory perspective, focusing on the COO in relation to operational resilience makes good sense.

Some of the key elements relevant to OR fall squarely within the COO's remit, and having an individual to hold to account for what a firm is required to do adds leverage to the regulatory approach (to which Mr Abacha at TSB can testify).

In that context, the challenge for COOs is how to discharge their responsibilities - especially when, at many firms, there remains (too) much to do before the DORA and FCA/PRA deadlines in Q1 2025: what might 'reasonable steps' look like?

Having a credible plan, with timeline and resources aligned, is clearly at the heart of the matter - even if that plan necessarily stretches beyond March 2025. And whilst there are many elements which COOs will need to cover for their firm's plan to get over the 'reasonable steps' hurdle, here I want to highlight just a couple of points.

**First, getting the balance right between the 'what' and the 'how':** yes, an effective risk framework is essential - but how will it work in practice? For regulators and firms, it's often the case that there's nothing as good as a crisis for breaking down silos across a firm and engendering truly effective collaboration.

The challenge is to embed those benefits sooner than at a crisis point. So, how does the culture of a firm enable the risk management framework to be truly effective? COOs are uniquely well-placed to see both sides of that coin - the design, implementation and governance of an effective risk management framework addressing operational resilience in all its guises, and the behaviours within the firm which can either bring the framework to life effectively - or the opposite.

So a supervisor's questions in relation to operational resilience will not just be about the process and the framework - but also about the firm's culture, and how the COO satisfies themself that the behaviours of staff - both senior and junior - will enable the framework to deliver what it is intended to deliver.

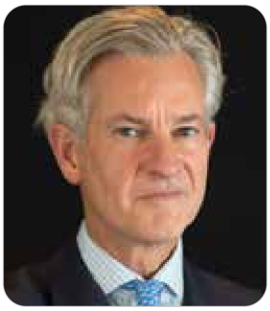
**Second, AI: is AI part of the challenge or part of the solution?** Most likely it's both. But firms are in different places on the 'AI use' spectrum; that is fine, but having a clear AI roadmap will be crucial - particularly one which reflects the realities of the firm.

In the UK, the FCA has said not only that it is looking to make greater use of AI - but also that, if firms aren't also thinking about how best to use AI, they risk the regulator knowing more about the firm than the firm's senior management knows. Whilst that is not intended to be a dictat for blindly using AI, it is a clear indication that firms should be mindful of how gen AI can effectively help firms - and COOs - in managing operational resilience more effectively.

**Finally, from a regulatory perspective operational resilience is not a passing fad:** new requirements, around the world, have been years in the making and implementing - and, whilst there are some specific milestones coming up, regulatory focus will remain after those particular milestones have passed.

That is not just because, for many firms, implementation will take longer than the time remaining, but also because of the impact on firms - and on the economy and society more generally - if banks do not effectively address operational resilience. And for COOs that means that they will be in the regulatory spotlight for some time to come.

# Leading Resilience



**Stuart Tootal**

Armstrong Wolfe Alliance Partner

Matero Management Consultancy

# Decision making in crisis and business culture

In 1971 Graham Allison published ‘the Essence of Decision’, analysing the decisions taken by Kennedy’s administration during the 1962 Cuban Missile Crisis.

Allison’s book contended that rational intentions to act against the Soviets, while avoiding the risk of a nuclear war, were nearly confounded by the influence of decision-making factors beyond JKF’s control. Allison argued that non-rational factors, such as organisational bureaucracy, cognitive bias, and politicking risked the unintended consequence of a nuclear exchange, which Kennedy was studiously trying to avoid. In essence middle management almost failed to exercise his intent.

Writing a century before Khrushchev’s near fatal decision to deploy missiles in Cuba, Helmuth von Moltke also theorised about the intent of strategy and the reality of executing decisions, when he stated that no plan, however well crafted, withstands actual contact with realities.

Von Moltke claimed that the factors like chance, bad weather, and misunderstandings were the frictions of reality on a battlefield, which militated against a strategy unfolding as it had been intended. Speaking about conflict a little closer to this century, Mike Tyson put it more succinctly. When talking about his impending heavyweight fight with Evander Holyfield in 1996, he said, ‘Everyone has a plan until they get punched in the mouth.’

Whether the 2008 financial crisis, corporate scandals, Covid, or just BAU, it does not take an academic, 19th Century Prussian general, or heavyweight boxer to tell us that the best laid plans often go astray when they meet the reality of actual circumstances.

Corporations are full of talented people and the challenge is not lost on today’s business leaders. Published in 2001, David Norton and Robert Kaplan’s book, ‘The Strategy Focused Organisation’, surveyed 200 top global companies and stated that nine out of ten corporate strategies failed, citing that the ‘execution gap’ was the number one concern of most CEOs.

Twenty years on the situation has been exacerbated by the increasing frequency of Black Swan events and the need to operate in a near perennial crisis environment. The issue is how you plan for uncertainty and make decisions, when the frictions of reality, whether external or internal to an organisation, often conspire to militate against the execution of strategic intent.

Companies talk about compliance measures, risk oversight structures, and crisis playbooks. However, the associated proliferation of committees and lines on a Gantt chart does not equate to decision-making for the unexpected or an ability to pivot and deviate appropriately when the frictions of reality collide with the intentions of strategy.

If anyone thinks ‘Agile’ project management is a panacea, a quick Google search provides a different view. A conservative estimate of available statistics indicates that 60-70% of Agile programmes fail.

Organisations may emphasise the importance of delegating authority and having the right culture to empower staff to exercise initiative and respond to events as they unfold at the coalface. But culture is not about cascading executive endorsed Power Point slides or occasional and expensive offsites, where teams talk of empowerment before promptly returning to the existing status quo of foot dragging practices in their workplaces.

Consequently, it is likely that senior management will continue to decry the 'frozen middle' and a propensity for every decision to be delegated upwards in their organisations.

Organisational culture is about the way a collective group and individuals behave on behalf of the institution they are part of. Culture is most notable, good, or bad, in times of change, complexity, uncertainty, and crisis. Consequently, it is about the decisions and resulting actions people and bodies chose to make; especially when they are under pressure.

However, if culture is to extend beyond empty value statements and a rain forest of compliance policy and regulations, it must be centred on decision-making method. Without a codified decision-making methodology, applied across every function and at every level, logic indicates that culture may be an empty vessel in many organisations.

It is a situation that extends beyond crisis situations. Most companies claim to invest in their culture, yet many have a dismal record of customer complaints, which is an indicative mismatch between aspiration and actuality. An inability to address customer grievances and poor service in a timely manner, as near to the point of origin as possible, largely stems from a lack of empowerment at the frontline interface.

We have all been there when faced with an issue that appears relatively straight forward to address. When we finally get through to a customer relationship manager, we are exasperated to discover that the person we are speaking to is not a decision-maker and lacks the authority or knowhow to deal with the issue.

Instead, we are put on hold, referred to a supervisor or another department, resulting in inevitable resolution delay. The relationship is at best damaged, customer retention risked, and the costs remediation are likely to increase.

At a higher level, the inability to close the execution gap and its link to the delta in decision-orientated culture is exacerbated by the vagaries and fragilities of human behaviour. Seventy years of behavioural economics tells us that people are naturally poor intuitive data analysts. Most people have an innate preference for gut feel and making 'comfortable' decisions, which fit their preconceptions of a situation.

**"Organisational culture is about the way a collective group and individuals behave on behalf of the institution they are part of."**

They do so at the expense of ignoring statistics and intelligence, which may not fit their version of reality. They are also influenced, by cognitive bias, accepting the familiar, and succumbing to social pressures, such as group think or what the boss thinks. In short, a range of biases, conscious or subconscious, which exacerbate the frictions of execution when the rubber of intent hits the reality of the road.

In the last decade, the credit crisis, pace of technological change, proliferation of market disrupters, increasing conduct scrutiny, Covid and now inter-state war in Europe and the Middle East, should have taught businesses that they need get used to the unfamiliar, uncomfortable, and the uncertain.

The need to make decisions under pressure, which empower people and make them resilient to friction execution is a constant requirement. The essence of the solution lies in the art of decision-making schooling and method, with the empowerment it offers if embedded at all levels of an organisation, from the macro to the micro.

While strategic decision and design should incorporate contingencies for the unexpected, which reduce random and bias, those who deliver them at the more tactical echelons also need to be properly empowered to act within intent.

This requires decision-making to be taught throughout an organisation, so that it delegates authority to decide, act appropriately, and pivot as required when planning aspirations and reality diverges.

Decision-making R&D exists in the academic, sporting, and military arenas, with actual application most marked in the latter field. With some notable specific exceptions, in the aviation sector and Formula 1, it is considerably less established in the commercial world.

How many companies can claim to have codified decision-making methodologies that transcend their organisations, which influence their purpose and performance through guiding the choices they and their people make at every level of an institution?

Given the current and future business environment, it is an urgent question that they need to address. Two years ago, Boris Johnson announced that he was considering improving the civil service performance by partnering with the military academy at Sandhurst.

It may have been an idea that did not see out his tenure as PM, however, it reinforced the contention that the military who have already spent years dealing with crisis and investing in an empowerment culture based on delegated decision-making, which has endured and proven itself throughout the turbulence of several decades, might have something to offer to the business community.

**“The need to make decisions under pressure, which empower people and make them resilient to friction execution is a constant requirement.”**

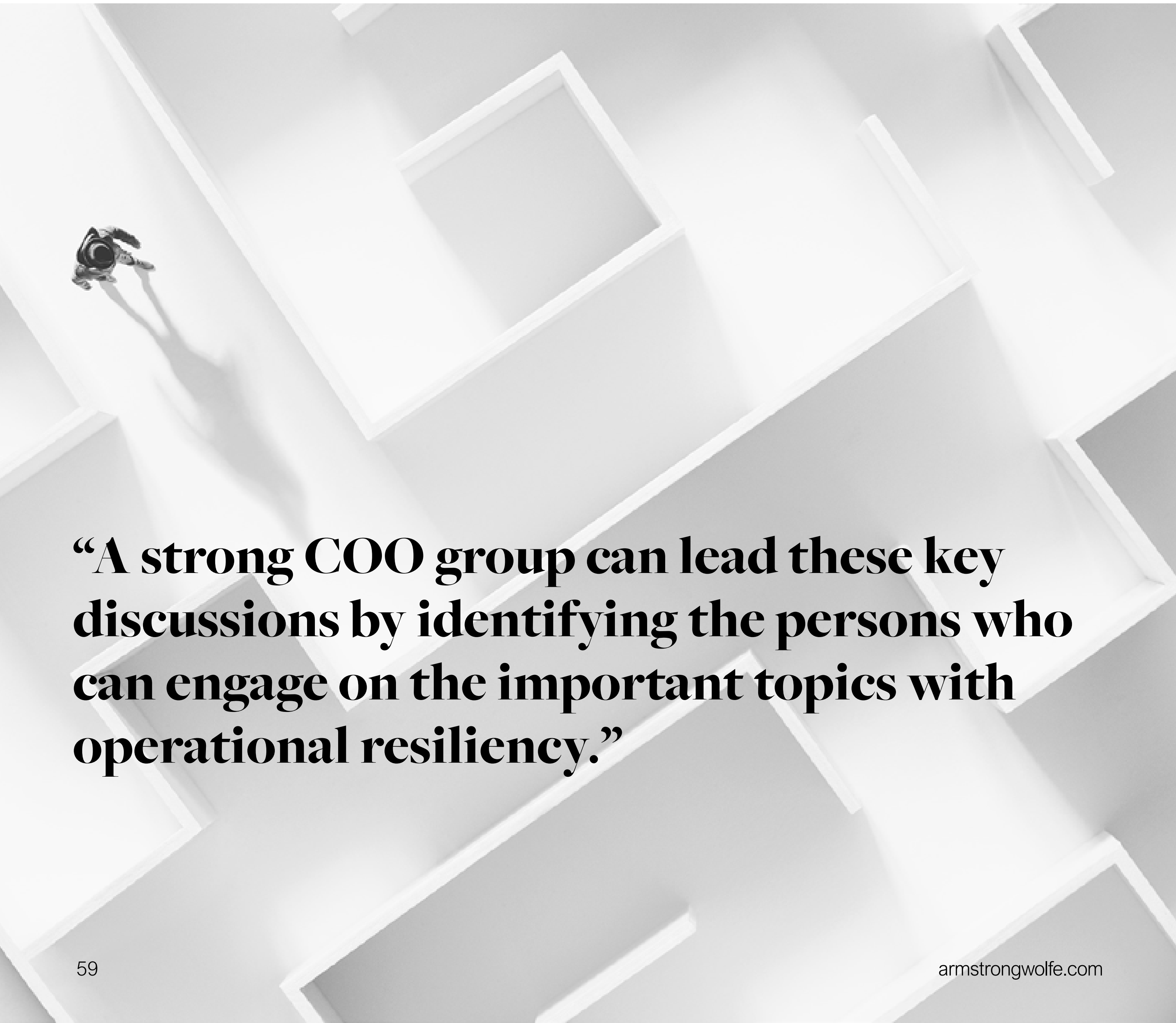
## Some questions below to frame key discussions:

1. Do we understand where the organization is today and where we need to be tomorrow?
2. How can we improve frameworks surrounding how to identify, catalogue, measure and manage those areas of improvement? Tactically, operationally and strategically?
3. Is the organization self-identifying areas of improvement in its lines of defence, with specifics and actions?
4. Does the organization have the ability to join the dots consistently?
5. Does senior management feel engaged in the resiliency process as part of the overall business objectives?

The most important reality for progress in operational resiliency is the commitment to establishing the framework's needed to understand the challenges of your organization.

This kind of commitment is underscored by beliefs and values. Aristotle recognized that the future is inherently uncertain and that human knowledge has limitations.

But a commitment to create these frameworks of connectivity will ensure successful leadership for those certain moments of uncertainty.



**"A strong COO group can lead these key discussions by identifying the persons who can engage on the important topics with operational resiliency."**

General Sir Peter Wall

Armstrong Wolfe Alliance Partner

CEO, Amicus

# We are witnessing the dawn of a new era in global geopolitics

The belligerent autocracies (China, Russia, Iran and North Korea) are striving for the upper hand over democracies across the world, with many former west-supporting nations remaining neutral or leaning the other way.

The wars in Ukraine and Gaza and threats from China to various causes, not least the integration of Taiwan to communist China, are symptoms of this geostrategic trend.

These vectors threaten the security of the west and the stability of the global economy; examples are the rise in energy prices and the vulnerability of supply chains. They impact us directly and affect all organisations from the public sector and large corporations to SMEs.

We should assume these pressures are here to stay. So we need an approach that allows us to manage their effects while we get on building our businesses and delivering our outputs. In addition to these external influences that we cannot control, we also have a range of shocks closer to home that can challenge our resilience.

These might include market forces, what our competitors are doing, the motivation and behaviour of our own people and how our customers see us. Such potential setbacks are ever-present and our success will depend on how we handle them, as and when they occur. How we respond to them will demonstrate the resilience of our business or operation.

A useful definition of operational resilience is 'the ability to prevent, handle, and learn from disruptive events'. Let's take those three actions in turn.

Most businesses see prevention of disruptive events through the way they manage risk. Indeed, many organisations organise their board and executive committee activity primarily around the management of risk; they want to horizon scan, foresee what can go wrong and create contingency plans that give confidence they have a method of handling those shocks and setbacks.

This is first base for developing resilience and it is essential, but not sufficient; because it is limited by our ability to anticipate risk, by our ability to imagine the worst things than can happen. As an example the UK had contingency plans for a pandemic, but not for the type that turned up.

Handling crises is always a bit of a shock, but people raise their game and rally around. Many organisations have told us that they feel they rise to the challenge, the adrenaline flows, and they are more creative and resolute than in steady state.

Much of this depends on the conduct of their leaders. If they can hold it together and ‘keep their heads, when others are losing theirs,’ as the saying goes, then there’s hope we can muddle through. This gives confidence to the employees, customers and stakeholders.

There’s no doubt that crises are judged more by the way they are handled than by the initial failing or root cause.

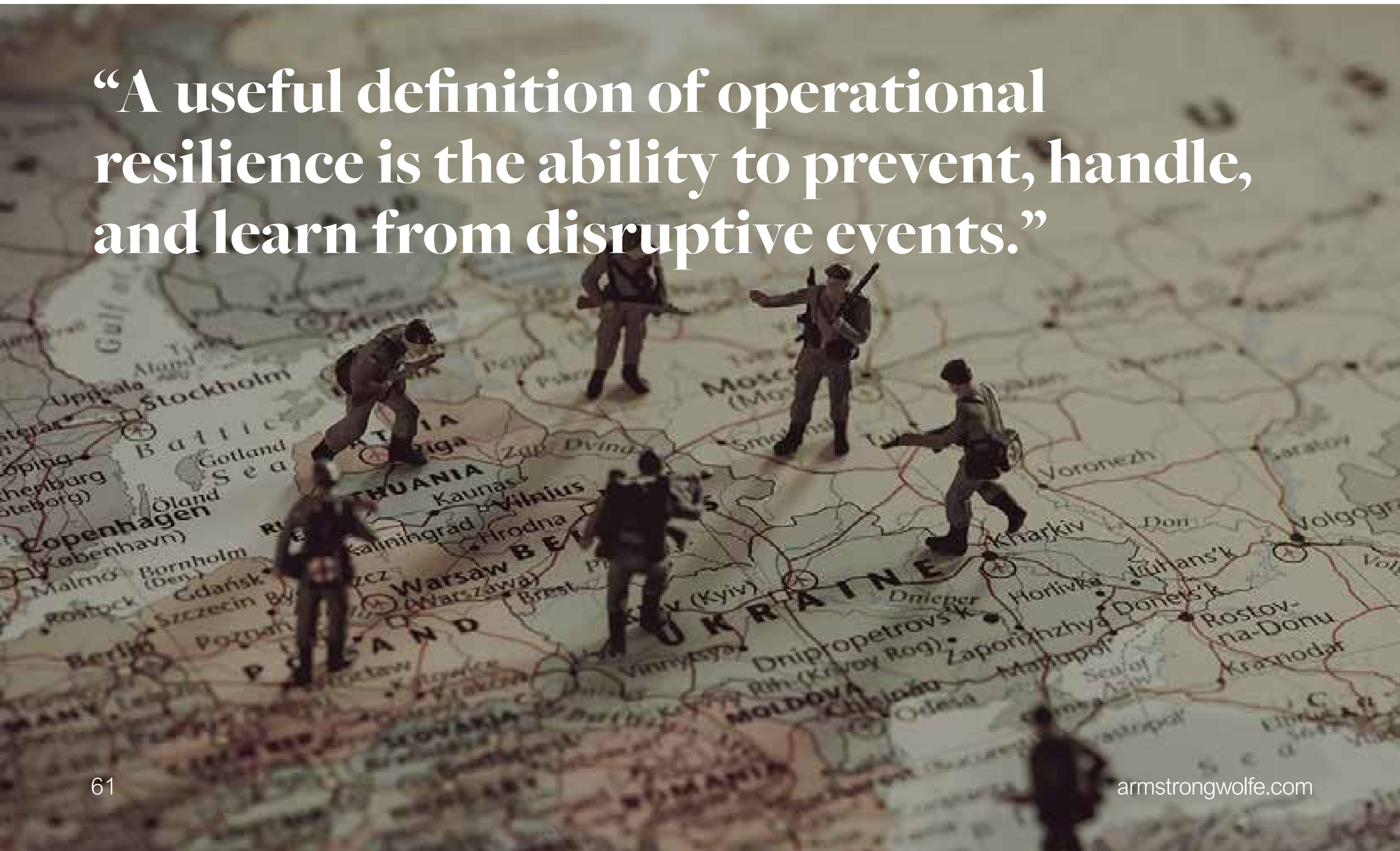
The senior leadership plays a key role in this – steadying the ship, supporting their teams throughout the business, communicating honestly and rejecting any notion of those cover-ups that both look insincere and are usually blown apart very quickly, thereby compounding damage to reputation, both internally and externally. The fact that so many organisations fail to get this right is really quite alarming.

Third we must look at learning from shocks and setbacks, whatever the cause. The best organisations confront these head-on, without fear or favour. Rather than looking for culprits or blame, they are intent on finding out what happened and how they can do better next time. Transparency is key, and if it is masked by people within the organisation, the prospect of repeat failures is grossly amplified. How many public enquiries are failing in their duty because they are more focused on the victims’ experiences and apportioning blame than improving leadership, systems and processes to prevent repeat occurrences?

The unifying issue around these points is mindset and mental resilience. Processes will never fully eradicate the impact of disruptive events, shocks or setbacks. The resilience of an organisation to withstand these challenges is down to the abilities of its senior teams, both collectively and as individuals, to cope with them robustly, no matter when or how they emerge.

It requires them to put everything else on hold, and come together to nail the solution, no matter how hard, or how long it takes, and regardless of the toll on them and their families. As senior leaders if you aren’t prepared for this eventuality, now is the time to think about it. Such crises are the moment when leadership is at an absolute premium. Those who pass the test emerge with reputations enhanced; the opposite certainly applies, and it can be brutal.

At Amicus we specialise in supporting senior executive teams to address these issues and develop the collective resolve and mindset to handle major setbacks. Operation CRUCIBLE is our crisis response training to condition the mindset of leadership teams. It will give you the confidence to step into the breach rather than step away. That’s the essence to leading the operational resilience of your business.



> “A useful definition of operational resilience is the ability to prevent, handle, and learn from disruptive events.”

# Alliance Partner Viewpoints

**Fahreen Kurji**

Chief Customer Intelligence Officer

Behavox

# AI Implementation from a Vendor's Lens: Insights and Strategies

In the rapidly evolving world of artificial intelligence (AI), understanding how technology is implemented from a vendor's perspective is crucial for grasping the broader impacts on industries, particularly in the financial services sector.

Equally important is the need for vendors to take advice from their customers and develop a deep understanding of their business needs and challenges. This holistic approach ensures that AI solutions are tailored effectively and deliver maximum value.

> *Interviewer: How do vendors begin the AI implementation journey with clients?*

**Behavox:** The first step involves a deep understanding of the client's business environment, challenges, and objectives. For a company like Behavox, specializing in compliance and security solutions, this means identifying specific operational risks such as insider threats, market abuse, and compliance breaches that the client needs to manage more effectively.

For example, the notorious Wells Fargo scandal highlighted the need for robust internal monitoring to prevent unethical behavior. Collaborating closely with clients helps us design solutions that address their unique requirements and concerns.

> *Interviewer: How do vendors tailor AI solutions to meet the specific needs of clients?*

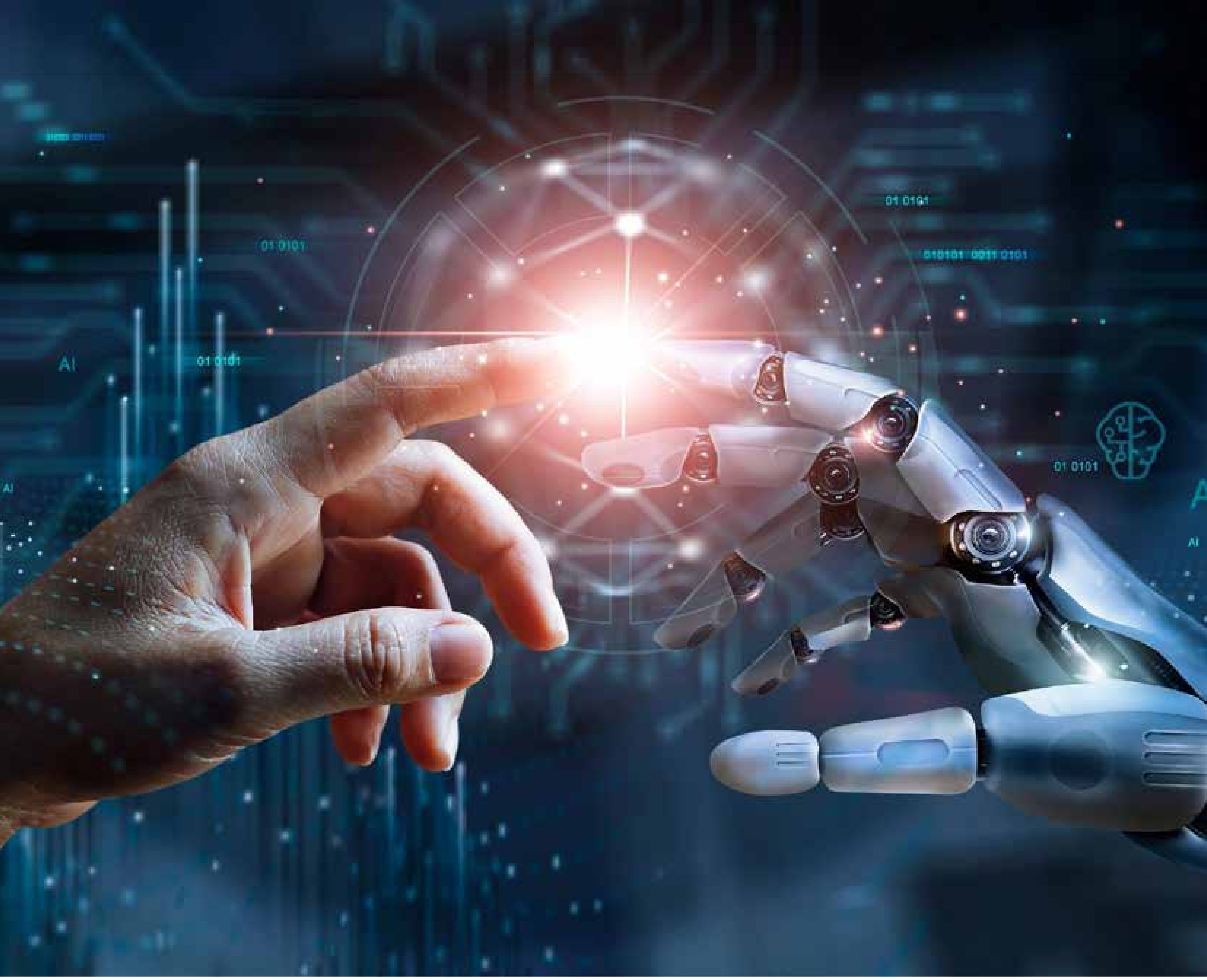
**Behavox:** Once the needs are clearly understood, the next step involves tailoring AI technologies to address these specific challenges. Behavox employs a suite of AI-driven products each designed to meet different aspects of compliance and risk management.

For instance, our Quantum platform uses AI to monitor and analyze communication for signs of unethical behavior, while our Falcon platform focuses on human risk management by predicting and mitigating risky human behaviors. This approach was instrumental in detecting fraudulent activities in the case of the LIBOR scandal.

> *Interviewer: What are the challenges of integrating AI solutions with existing systems, and how are they overcome?*

**Behavox:** Integrating AI solutions into a client's existing IT and operational infrastructure is one of the most challenging phases of the implementation process. Behavox ensures that its solutions can seamlessly integrate with existing data systems and workflows without disrupting ongoing operations. This integration is critical for maintaining data integrity and operational continuity.

For example, during our implementation with a major European bank, seamless integration was essential to avoid disruptions in their daily operations.



> *Interviewer: How important are training and onboarding in the AI deployment process?*

**Behavox:** Deploying AI is not just about technology integration; it also involves significant human elements, particularly training and onboarding. Behavox invests in comprehensive training programs and documentation to ensure that all users are proficient in utilizing the new systems.

This includes helping clients understand how AI makes decisions, thus aligning with the explainable AI principles that Behavox upholds. Our training programs have proven effective, as seen in our work with large financial institutions that need to quickly adapt to new regulatory requirements.

> *Interviewer: What are some of the regulatory challenges vendors face during AI implementation, and how are they addressed?*

**Behavox:** One of the biggest challenges AI vendors face is the complex regulatory environment of the financial sector. Behavox uses its regulatory expertise and its Intelligent Archive solution to help clients navigate these complexities, ensuring compliance with international laws and regulations.

For instance, regulatory requirements such as MiFID II in the EU demand detailed records of communications, which our solutions effectively provide.

> *Interviewer: How do vendors ensure data privacy and security in AI implementations?*

**Behavox:** As AI systems often handle sensitive data, ensuring privacy and security is paramount. Behavox addresses these concerns through high-security standards, detailed access controls, and SOC II-certified environments, thus reassuring clients about the security and confidentiality of their data. Our robust security measures have been particularly crucial in environments dealing with sensitive financial data, such as during our deployments in major investment banks.

> *Interviewer: How do vendors ensure that AI solutions are scalable and adaptable to future needs?*

**Behavox:** AI solutions must not only meet current needs but also be scalable and adaptable to future changes. Behavox's AI solutions are designed to evolve, supporting over 46 languages and capable of adapting to new regulatory and operational requirements as they arise. This adaptability was essential in our partnership with global financial firms that operate across multiple jurisdictions with varying regulations.

> *Interviewer: How do AI implementations enhance productivity and efficiency in financial firms?*

**Behavox:** By automating routine tasks and providing advanced analytical capabilities, AI allows firms to focus on higher-value activities, thus boosting productivity and operational efficiency. For example, our AI solutions have enabled financial analysts to concentrate on strategic decision-making rather than getting bogged down by repetitive data analysis tasks.

> *Interviewer: How do AI solutions provide comprehensive risk management?*

**Behavox:** Behavox's AI solutions provide comprehensive coverage of potential risks, from compliance to insider threats, enabling businesses to proactively manage and mitigate these risks before they escalate. An example is our work with firms subject to stringent anti-money laundering regulations, where our AI effectively identifies suspicious activities early.

> *Interviewer: How do vendors build trust among stakeholders through AI implementation?*

**Behavox:** By ensuring compliance and protecting against operational risks, AI implementation by vendors like Behavox plays a crucial role in building trust among stakeholders, including investors, regulators, and the public. Our transparent AI models and rigorous security standards have been pivotal in gaining confidence, as demonstrated in our collaborations with top-tier financial institutions.

From a vendor's perspective, implementing AI in the financial services sector is a multifaceted process that requires deep industry knowledge, technological expertise, and a clear understanding of regulatory environments. Behavox exemplifies how vendors can successfully deploy AI to meet their clients' diverse needs and enhance their capability to manage risks and comply with regulations. As AI continues to evolve, its implementation by vendors will remain a critical factor in the digital transformation of industries.

**"Integrating AI solutions into a client's existing IT and operational infrastructure is one of the most challenging phases of the implementation process."**

**Chris Rigg**

Armstrong Wolfe Alliance Partner

Global Economics Group

# How should banks think about operational resilience?

Operational resilience refers to a bank's ability to withstand and recover from disruptions that threaten its critical operations. It's a multi-faceted concept encompassing prevention, adaptation, and recovery, ensuring continued service delivery despite challenges.

A key element of improving your operational resilience is to understand and evaluate your current operating model by asking key questions:

1. How are the operational requirements of the business changing?
2. How do we meet the increased expectations of the regulators?
3. How do I better leverage technology advancements like AI and automation?
4. Do I have the right talent to achieve our objectives?

These questions help guide your thinking and determine if traditional transformation levers can raise your performance to the expected level while keeping run rate costs at a level that doesn't degrade profitability.

Assessing the resiliency of your operating model requires understanding the expectations and requirements of the different stakeholders, including management, customers, and the regulator.

Banks should approach operational resilience from a holistic perspective, including:

**Understand the Potential for Disruption and where it can come from**

- Operational resilience acknowledges that disruptions are inevitable. These disruptions can be external (natural disasters, cyber attacks, pandemics) or internal (system failures, human error).
- The aim is not just to react to disruptions but to proactively prepare for various scenarios, thereby minimizing their impact on core banking functions.
- While operational risk management is a crucial component, resilience goes further. It involves a holistic approach considering people, processes, technology, and infrastructure.

**Build and Maintain Capabilities that Increase Resilience**

- **Preventative Measures:** Proactive steps to identify and mitigate potential risks before disruptions occur.
- **Adaptive Capacity:** The ability to quickly adjust operations and processes in response to disruptions.
- **Recovery Time:** Minimizing the time it takes to restore critical functions after a disruption.
- **Learning and Improvement:** Analysing past disruptions improves resilience and prevents future occurrences.

### Assessing Performance from an Operational Resiliency Perspective

Understanding your business and operating model's current resiliency is critical to establishing the target state and understanding the gap to achieving it.

The key areas to include in your assessment include:

1. **Business Continuity Plan** (BCP) - Is your BCP well-defined, comprehensive, tested, and updated regularly?
2. **Risk Framework** - Does your current risk framework identify, assess, and mitigate potential disruptions to the business?
3. **Culture** - Do you have a continuous improvement and innovation culture that can adapt to changing business needs, market conditions, and regulator expectations?
4. **Leadership** - Does the leadership team have the necessary skills and experience to manage the operations and achieve resiliency objectives?
5. **Track Record** – Does the organization have a strong track record of success in responding to past disruptive incidents?
6. **Process Design** - Are critical business processes designed to minimize disruption from incidents?
7. **Customer Expectations** – Are your customers' performance quality expectations factored into your business recovery plans?
8. **Technology** – Can your technology infrastructure withstand disruptions and maintain service continuity?
9. **Third Parties** – Do you have a strong vendor management program that monitors performance and ensures critical vendors can maintain service quality during disruptive incidents?
10. **Organization** - Is the organization aware of your resiliency requirements? Are they trained on your resiliency strategy? Do they regularly participate in practice exercises?

### Leveraging AI to Increase Operation Resilience

AI (Artificial Intelligence) offers a powerful toolkit for banks to bolster their operational resilience, including:

**Enhanced Risk Detection and Management:**

- Machine Learning (ML) algorithms can analyse vast amounts of data to identify patterns and anomalies that might signal potential disruptions, including cybersecurity threats, fraudulent transactions, or operational glitches.
- AI-powered systems can continuously monitor activity and learn over time, becoming more adept at predicting and preventing issues before they escalate.

**Proactive Scenario Planning and Stress Testing:**

- AI can simulate various disruptive scenarios, such as cyber attacks or economic downturns. Banks can identify vulnerabilities and develop contingency plans to ensure business continuity by analysing potential outcomes.
- AI can automate stress testing processes, allowing banks to run more frequent and comprehensive simulations, leading to a more robust understanding of their risk profile.

**Improved Decision-Making and Resource Allocation:**

- AI can analyse historical and real-time data to provide insights for better decision-making during disruptions, including optimizing resource allocation, prioritizing tasks, and implementing effective recovery measures.
- Predictive analytics powered by AI can help banks anticipate resource needs during disruptions, allowing them to pre-emptively allocate staff and resources to critical areas.

**Streamlined Operations and Automation:**

- AI-powered automation can streamline routine tasks and free human resources to focus on more complex issues during disruptions, including automated customer service chatbots to maintain customer support even during system outages.
- Automating repetitive tasks also reduces the risk of human error, further enhancing operational resilience.

**Operational resilience can be a surprising differentiator in today's competitive banking landscape, including:**

Enhanced Customer Confidence:

- Frequent disruptions can erode customer trust. A resilient bank that minimizes downtime and maintains service availability fosters trust and loyalty.
- Customers are increasingly aware of cyber threats and value banks that prioritise data security and can recover quickly from cyber attacks.

**Improved Operational Efficiency:**

- Resilient banks can proactively identify and mitigate risks, streamline operations, and avoid costly disruptions, which translates to cost savings and improved efficiency.
- Resilient banks can more easily adapt their processes to changing regulations or market conditions, making them more agile and responsive.

**Innovation and Growth:**

- A strong foundation of operational resilience empowers banks to take calculated risks and invest in innovative technologies and services.
- Knowing they can bounce back from setbacks allows banks to experiment with new offerings and seize growth opportunities without being overly risk-averse.

**Attracting and Retaining Talent:**

- A resilient bank that prioritises employee preparedness and safety during disruptions fosters a more positive work environment - creating a significant advantage in attracting and retaining top talent.
- Investors are increasingly looking for resilient institutions. A solid operational resilience posture can improve a bank's creditworthiness and attract more favourable investment opportunities.

Overall, operational resilience is not just about mitigating risks; it's about building a foundation for sustainable growth and success in a dynamic and competitive financial landscape.

> **"Banks can navigate challenges confidently, inspire trust, and ultimately outperform their less resilient competitors by prioritizing resilience."**

Financial Services

GEG CONSULTING

*A Division of Global Economics Group, LLC.*

We are industry veterans with decades of experience who have helped banks successfully navigate historic regulatory and economic upheavals. We see new and unprecedented **Regulatory Challenges** wrought by technological changes in a volatile economy. We want to help our People and Clients succeed by Collaborating on solutions that address risk, compliance, and operational challenges.

We provide **high-value consulting** services, leveraging a uniquely experienced and efficient network of experts and partners, to financial services companies—banks, broker-dealers, asset managers, and insurance companies—across the first, second, and third lines of defense. Our services address the regulatory, people, process, technology, and data challenges that ultimately affect our clients' ability to succeed. Our delivery resources consist of GEG professionals and key alliance partners experienced in helping banks meet regulators’ expectations.

**Harry Toukalas**

Armstrong Wolfe Alliance Partner

Co-Founder and CEO, Swarm Dynamics.

# The intertwined dance of culture and technology: building a foundation for operational resilience

The landscape of operational resilience is constantly evolving, demanding a dynamic interplay between organisational culture and new technologies.

This interplay is not a competition, but a powerful synergy. In this regard, culture lays the groundwork by fostering a resilient mindset while driving collaboration. Technology, in turn, provides the tools to amplify this cultural foundation, offering deeper insights and automation capabilities. Only by harmonising these two elements can organisations build a better standard of operational resilience.

## Culture: The Bedrock of Resilience

The cornerstone of a resilient organisation lies in its culture. Organisations cannot build true operational resilience through policies and frameworks alone. Therefore, leadership must set the tone, championing resilience as a core value and integrating it into decision-making at all levels. This 'tone from the top' approach dispels the notion of resilience as a mere compliance exercise, elevating it to a fundamental operating principle. The COO is well placed to take the lead in this regard.

But it doesn't stop there because while the tone from the top is critical, culture is ultimately a local construct. It mainly forms and spreads at the local team level where people interact and connect on a daily basis.

To this end, resilience becomes stronger through a seamless collaboration across various departments. Silos must be broken down, fostering cross-functional teamwork between operations, technology, risk management, security, and business continuity.

Open communication, knowledge sharing, and a sense of collective accountability for resilience are also essential, while strong governance structures can facilitate this interdepartmental coordination, ensuring everyone is aligned towards a common goal.

Building a culture of psychological safety is equally crucial. Employees must feel empowered to surface potential risks and vulnerabilities without fear of reprisal. Fostering open communication is key, allowing for proactive identification and mitigation of issues before they snowball into disruptive incidents.

Finally, a culture that continuously strives to anticipate threats, identify vulnerabilities, and refine resilience controls is paramount. This necessitates a 'risk mindset' where learning is prioritised.

Therefore, organisations must promote a culture of learning agility, where employees actively participate in training, post-incident reviews, and the ongoing evolution of resilience playbooks based on simulations and real-world experiences.

## Technology: Empowering Resilience

A strong cultural foundation provides the platform for technology to work properly. Artificial intelligence (AI) and advanced analytics offer the potential for unprecedented insights into an organisation's operations, supply chains, and third-party ecosystems.

These technologies can detect patterns, anomalies, and potential failure points that human analysis might miss because appropriately trained algorithms are better at recognising patterns in vast amounts of data compared to humans.

However, unlocking the full potential of AI also requires a data-driven culture. Employees need to be able to trust the insights gleaned from AI-powered risk modelling, scenario planning, and predictive analytics, complementing traditional methods such as surveys and opinion-based red/amber/green risk dashboards.

This is not to imply that new technologies should replace traditional methods. Rather, they should be seen as the critical 'missing piece' to a comprehensive analytical approach to operational resilience.

Traditional analytical approaches such as surveys tell you what people think. New AI based technologies analysing, for example, digital trace data, tell you what people actually do. Both are important and should be considered mutually inclusive.

When incorporating various employee communication channels as part of the analysis, the privacy of employees can continue to be protected by confining the analysis to meta-data only (e.g. From-To-CC) rather than the text body of emails while overlaying anonymisation techniques.

AI-powered simulations can further bolster resilience by rigorously stress-testing plans against plausible threat scenarios. These simulations identify weaknesses and allow for proactive mitigation strategies.

However, their effectiveness hinges on a culture of continuous learning. Active staff participation in simulations, providing feedback, and iterating resilience protocols based on gained knowledge are all crucial for ongoing improvement.

As AI increasingly automates processes, cultural considerations take on added importance. Organisations will need to be able to foster trust in human-machine collaboration models, establish clear governance around AI decision-making authorities, and ensure staff feel comfortable with increased process automation.

Consequently, building an 'AI-augmented workforce resilience' may necessitate a certain level of reskilling and development programs to bridge the gap between human and machine capabilities.

> **"AI-powered simulations can further bolster resilience by rigorously stress-testing plans against plausible threat scenarios."**

Furthermore, AI can optimise resilience in several critical areas – real-time operational monitoring, automated response workflows, efficient resource allocation during disruptions, and robust third-party risk management. However, maximising the value of these functionalities requires a cultural shift.

Organisations need to embrace technological innovation, be willing to revamp legacy workflows to accommodate automation, and cultivate an environment of accountability across the entire enterprise. Ultimately, a culture that is based on a healthy level of faith in data-driven decision-making is essential for leveraging AI effectively.

## The Power of Synergy: Culture and Technology Working in Tandem

The true strength of AI for operational resilience emerges when its implementation is aligned with an organisational culture designed to amplify its impact. To this end, resilience must transcend being a purely technological solution and be ingrained into the organisation's DNA, becoming a collective mindset that permeates every level – from the boardroom to the control room.

## Building Resilience for the Future

As the pace of digital transformation accelerates and threats continue to evolve, organisations must harmonise their cultural and technological strategies. Leaders who champion resilience as a holistic, strategic imperative, while empowering their workforces with the right tools and fostering the necessary cultural traits, will create the environment for better practice operational resilience.

> **"Unlocking the full potential of AI also requires a data-driven culture."**

**Andy Nelson**

Armstrong Wolfe Alliance Partner

Head of Banking & Financial Markets, NTT DATA UK

# Operational resilience & cyber security: A COOs guide

## Enhancing Operational Resilience through Robust Cybersecurity Measures

Operational resilience has become a critical priority for Chief Operating Officers (COOs) across industries. In the financial services sector to maintain a stable financial system it has been mandated through regulation in the UK and currently in Europe the Digital Operational Resilience Act will apply from January 2025.

In an era where digital transformation is accelerating, the interdependence of business operations and technology has never been more pronounced.

This interconnectedness, while driving efficiencies and innovation, also exposes organisations to significant cyber threats. As such, cybersecurity is not merely a component of operational resilience; it is its cornerstone.

## The Imperative of Cybersecurity in Operational Resilience

Operational resilience from a cyber security perspective, refers to an organisation's ability to anticipate, prepare for, respond to, and recover from disruptions, ensuring the continuity of essential functions.

Cybersecurity threats, ranging from data breaches and ransomware attacks to insider threats and advanced persistent threats (APTs), represent a significant category of disruptions. Therefore, a robust cybersecurity strategy is integral to operational resilience.

COOs must recognise that the consequences of cyber incidents extend beyond IT. They can disrupt supply chains, compromise customer data, damage reputations, and incur substantial financial losses. Hence, integrating cybersecurity into the broader operational resilience framework is essential for safeguarding the enterprise's core functions.

> **"Operational resilience in the digital age is inextricably linked to robust cybersecurity measures."**

## Building a Cyber-Resilient Organisation

1. **Comprehensive Risk Assessment and Management:** A cyber-resilient organisation begins with a thorough understanding of its risk landscape. COOs should lead efforts to conduct comprehensive risk assessments, identifying critical assets, potential threats, vulnerabilities, and the potential impact of cyber incidents. This proactive approach enables organisations to prioritise resources and implement tailored security measures.
2. **Robust Incident Response and Recovery Plans:** Incident response plans are fundamental to operational resilience. COOs should ensure that these plans are not only well-documented but also regularly tested through simulations and drills. Effective incident response minimises downtime and mitigates damage, while well-defined recovery plans ensure a swift return to normal operations. Incorporating lessons learned from past incidents into these plans fosters continuous improvement.
3. **Investment in Advanced Cybersecurity Technologies:** Technology plays a pivotal role in defending against cyber threats. COOs should advocate for investment in advanced cybersecurity tools, such as artificial intelligence (AI)-powered threat detection, endpoint protection platforms, and Security Information and Event Management (SIEM) systems. These technologies enhance the organisation's ability to detect, respond to, and neutralise threats in real-time.
4. **Fostering a Security-First Culture:** Human error remains a significant vulnerability in cybersecurity. COOs must champion a culture of security awareness across the organisation. This involves regular training programmes, clear communication of security policies, and encouraging a proactive attitude towards cybersecurity. Employees at all levels should understand their role in protecting the organisation's digital assets.
5. **Third-Party Risk Management:** In today's interconnected ecosystem, third-party vendors and partners can introduce additional cyber risks. COOs should implement stringent third-party risk management processes, ensuring that partners adhere to the organisation's cybersecurity standards. Regular audits and assessments of third-party security practices are crucial for maintaining a secure supply chain.

## The Role of COOs in Cybersecurity Leadership

COOs are uniquely positioned to bridge the gap between operational resilience and cybersecurity. By taking an active role in cybersecurity initiatives, COOs can ensure that resilience strategies are comprehensive and aligned with the organisation's overall business objectives. Their leadership is vital in driving cross-functional collaboration, securing necessary resources, and maintaining a focus on resilience amidst evolving threats.

## Conclusion

Operational resilience in the digital age is inextricably linked to robust cybersecurity measures. As cyber threats continue to evolve in sophistication and frequency, COOs must prioritise cybersecurity as a foundational element of resilience strategies. By adopting a holistic approach that integrates risk assessment, incident response, advanced technologies, a security-first culture, and third-party risk management, organisations can build the resilience needed to withstand and recover from cyber disruptions.

In doing so, COOs not only protect their enterprises but also ensure financial services regulations are addressed to ensure sustained business continuity and competitive advantage in a volatile digital landscape.

> **"COOs can ensure that resilience strategies are comprehensive and aligned with the organisation's overall business objectives."**

- Over 100 former COOs available globally
- More than 3 millennium of combined experience
- Unlimited possibilities of value

# Armstrong Wolfe Interim

Bridge the gap, resolve the issue with SME resources

For more information contact **William Parry**
w.parry@armstrongwolfe.com

# Perceptions are people's realities they are framed by our five senses they are neither right or wrong but to be respected

Thank you for reading the perceptions of many

We hope they may further help shape your own

ARMSTRONG WOLFE™

# Interested in Armstrong Wolfe?

Join us: iCOOC, WCOOC and Ad Centrum.

Your voice can enrich the power of collective ambition.

info@armstrongwolfe.com

www.armstrongwolfe.com

ARMSTRONG WOLFE™

# Contact

Maurice Evlyn-Bufton
CEO Armstrong Wolfe
**maurice.evlyn-bufton@armstrongwolfe.com**

Piers Murray
Chief Operating Officer, US & Puerto Rico
**piers.murray@armstrongwolfe.com**

Terry Yodaiken
Global Head of Wealth & Asset Management
**t.yodaiken@armstrongwolfe.com**

Find us on LinkedIn: Armstrong Wolfe

Find us on LinkedIn: Women in the COO Community

ARMSTRONG WOLFE™