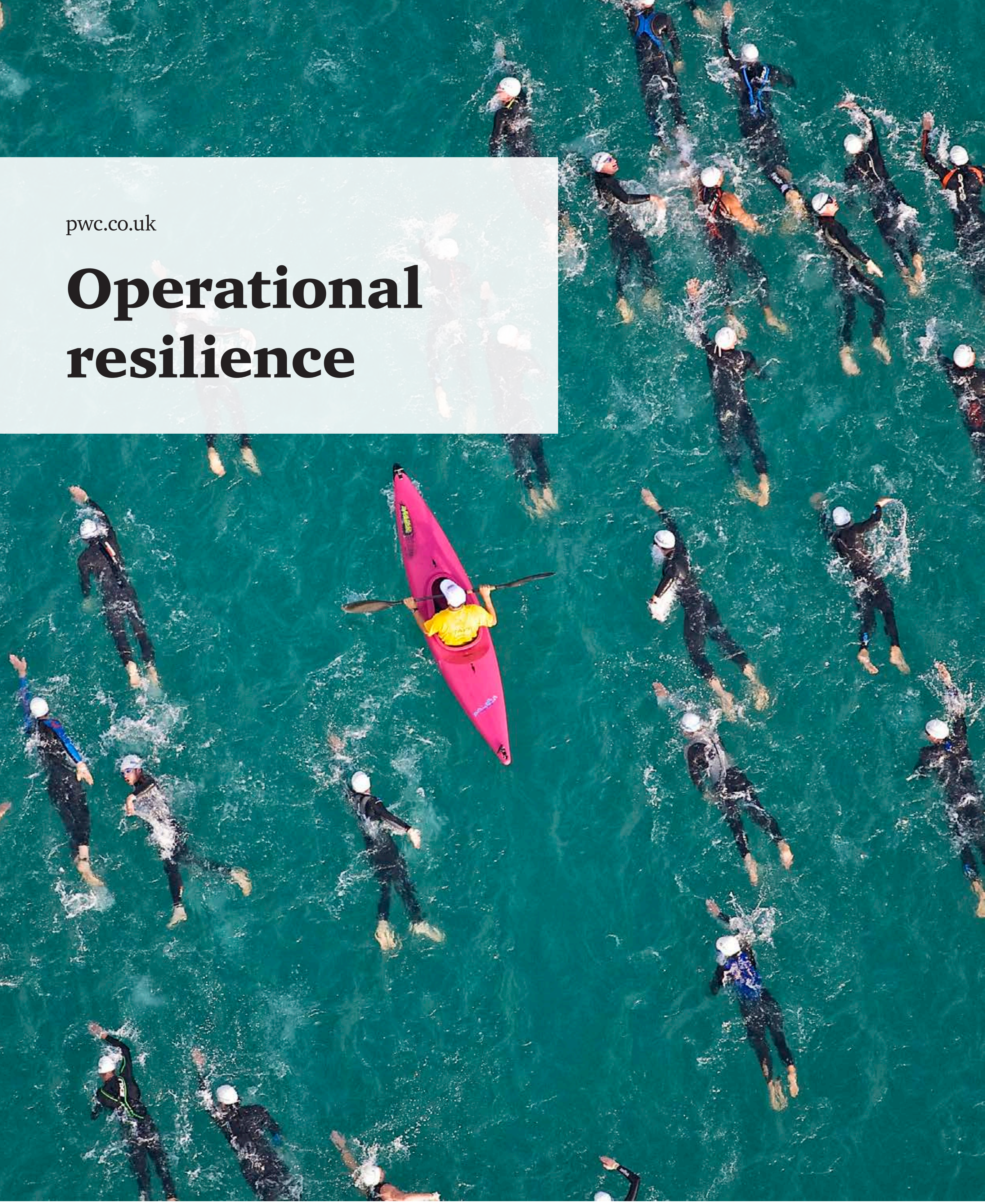
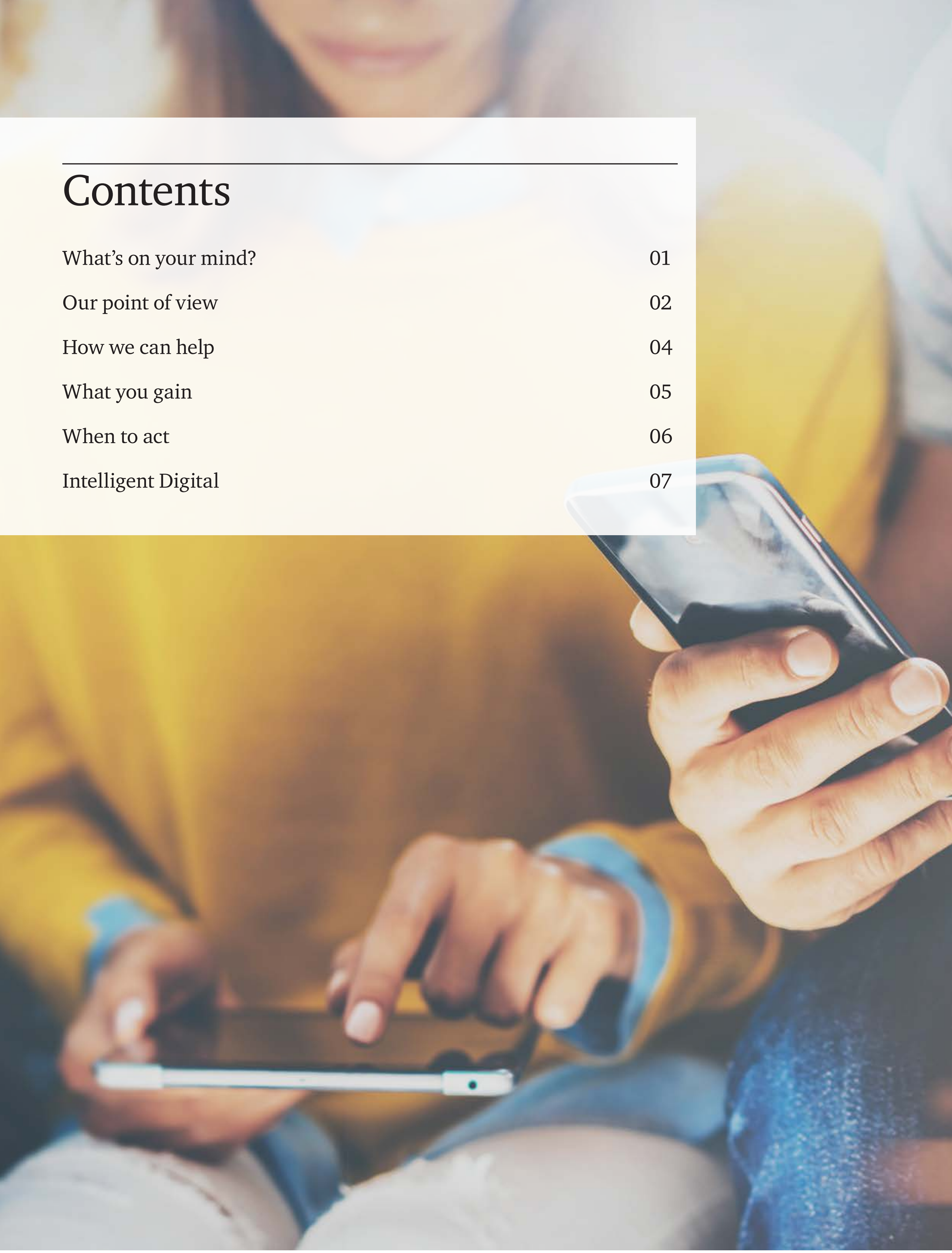
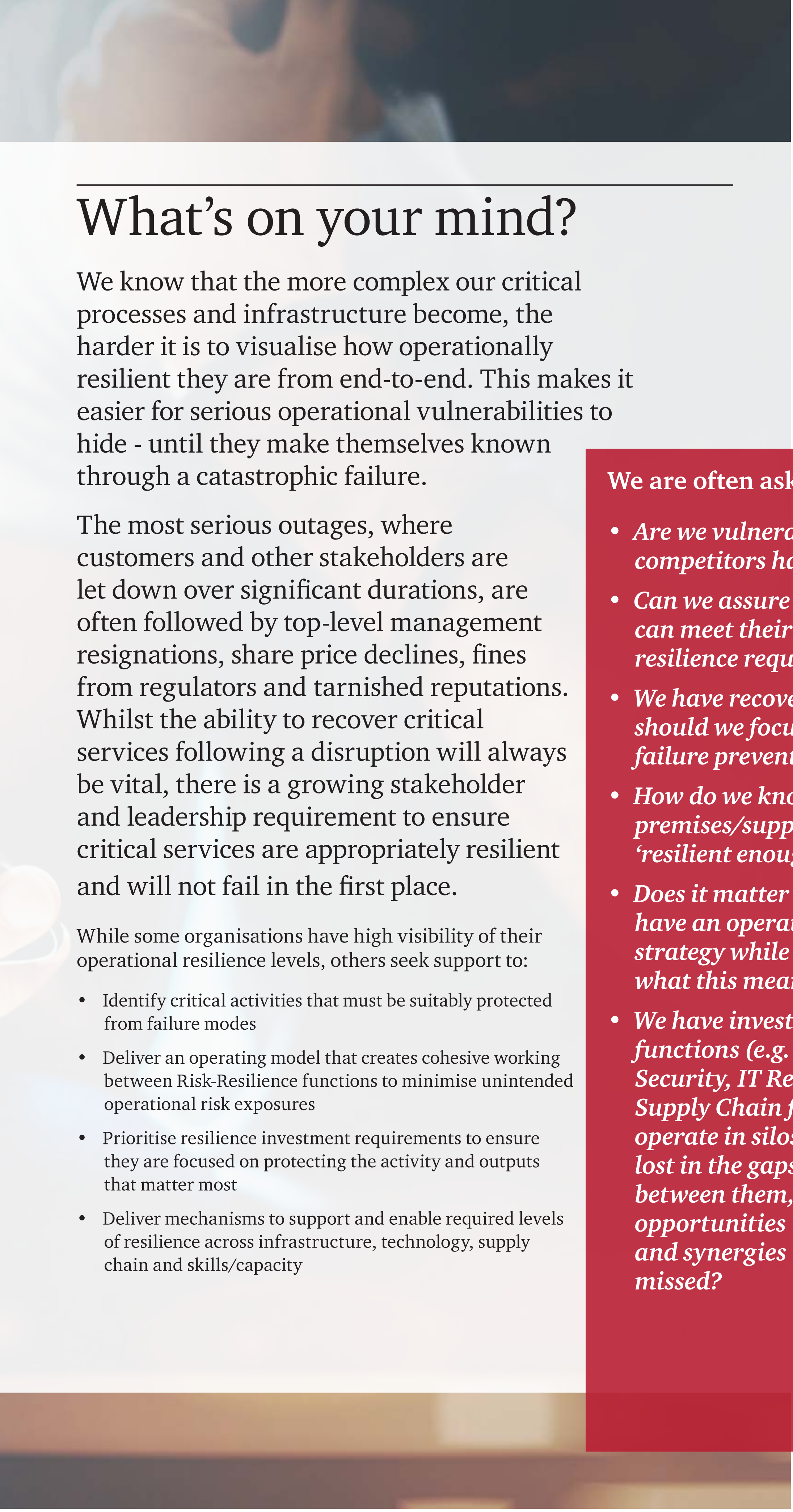
pwc.co.uk

Operational resilience



Contents





What’s on your mind?

We know that the more complex our critical processes and infrastructure become, the harder it is to visualise how operationally resilient they are from end-to-end. This makes it easier for serious operational vulnerabilities to hide - until they make themselves known through a catastrophic failure.

The most serious outages, where customers and other stakeholders are let down over significant durations, are often followed by top-level management resignations, share price declines, fines from regulators and tarnished reputations. Whilst the ability to recover critical services following a disruption will always be vital, there is a growing stakeholder and leadership requirement to ensure critical services are appropriately resilient and will not fail in the first place.

While some organisations have high visibility of their operational resilience levels, others seek support to:

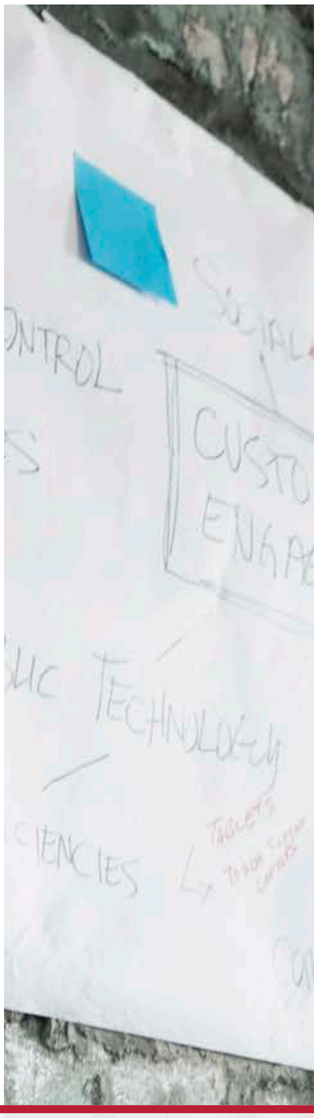
- Identify critical activities that must be suitably protected from failure modes
- Deliver an operating model that creates cohesive working between Risk-Resilience functions to minimise unintended operational risk exposures
- Prioritise resilience investment requirements to ensure they are focused on protecting the activity and outputs that matter most
- Deliver mechanisms to support and enable required levels of resilience across infrastructure, technology, supply chain and skills/capacity

We are often asked:

- *Are we vulnerable to outages that competitors have experienced?*
- *Can we assure our regulator that we can meet their increasing specific resilience requirements?*
- *We have recovery capabilities, but should we focus more on critical failure prevention?*
- *How do we know if our processes/IT/premises/supply chain/talent pool is ‘resilient enough’?*
- *Does it matter that our competitors have an operational resilience strategy while we are yet to define what this means to us?*
- *We have invested in Risk-Resilience functions (e.g. Risk, Continuity, Security, IT Resilience, Cyber and Supply Chain functions), but they operate in silos – will things get lost in the gaps between them, opportunities and synergies missed?*

Our point of view

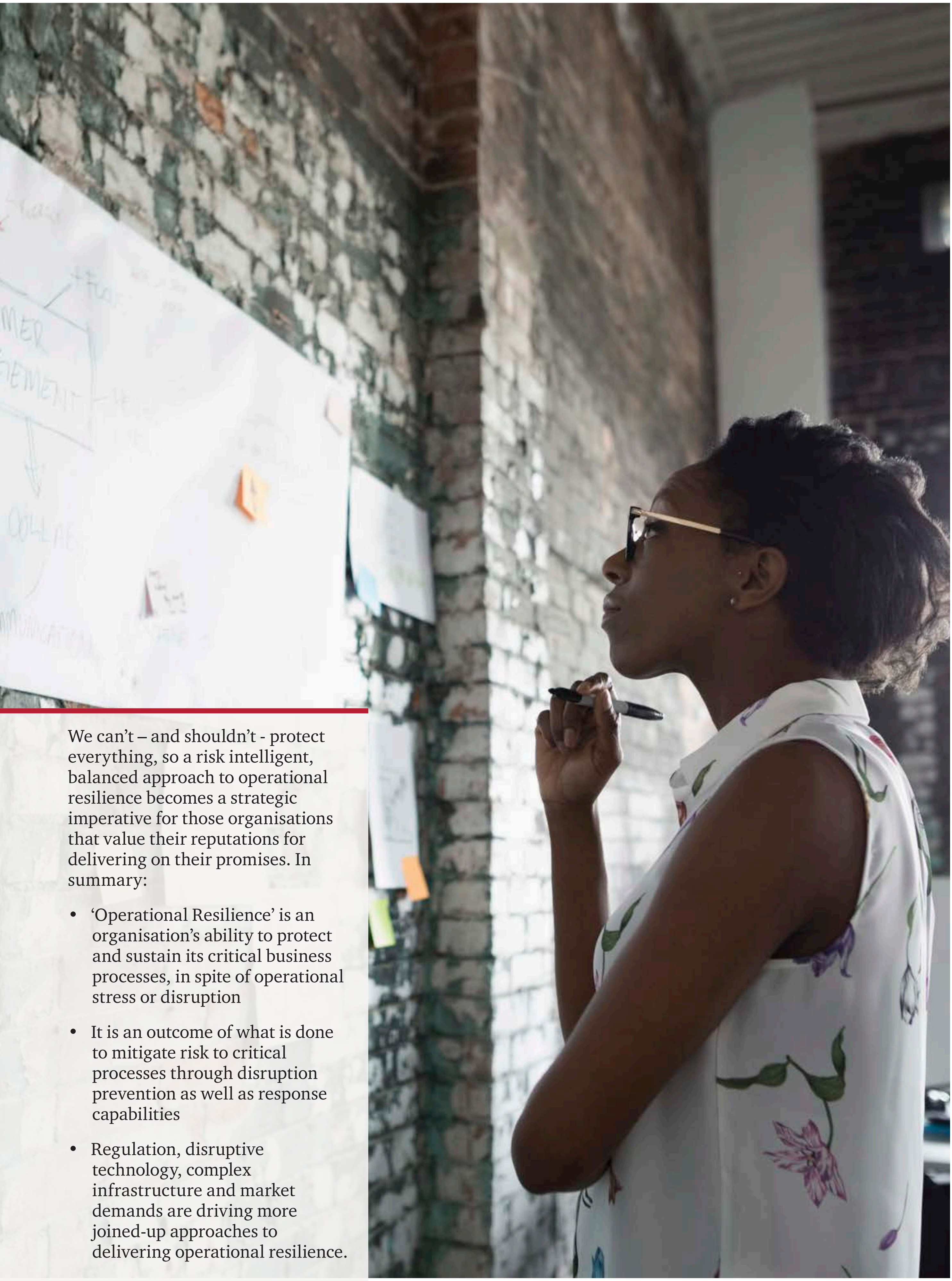
Organisational critical processes are dependent on an increasingly complex web of technologies, supply chains, critical assets, talent pools and infrastructure. Complexity makes it harder to effectively assess and monitor operational resilience, and resilience risks can only be aligned to the leadership's risk appetite when they are understood.



Findings following a major outage often include insights that while various discreet risks were understood in some areas of the business, the cumulative impact across end-to-end processes were not understood by the leadership or governance groups tasked with overall responsibility for ensuring critical operations are sufficiently resilient.

External stakeholders have become less forgiving of services that do not deliver what they promise when they are needed. Regulators are increasingly focused on ensuring that the most critical activity is not just recoverable, but protected from failure.

Whether an organisation is setting out to establish an Operational Resilience programme, ensure that the resilience (or lack thereof) of their critical processes is more visible, or address specific resilience issues within core areas such as IT, Supply Chain or Infrastructure, the approach must be aligned to the leadership's strategic objectives and risk appetite. Further, organisations with established risk-resilience functions that operate in silos should consider whether a lack of collaboration and understanding regarding strengths and weaknesses can fall between and contribute to the gaps. In these cases, it is likely existing investment can be optimised and efficiencies gained through more cohesive working across risk-resilience processes.



We can't – and shouldn't - protect everything, so a risk intelligent, balanced approach to operational resilience becomes a strategic imperative for those organisations that value their reputations for delivering on their promises. In summary:

- 'Operational Resilience' is an organisation's ability to protect and sustain its critical business processes, in spite of operational stress or disruption
- It is an outcome of what is done to mitigate risk to critical processes through disruption prevention as well as response capabilities
- Regulation, disruptive technology, complex infrastructure and market demands are driving more joined-up approaches to delivering operational resilience.

How we can help

Our operational resilience specialists can help your organisation to establish, refresh and maintain a more confident, efficient, embedded approach to Operational Resilience within your business-as-usual processes. Our services include innovative but sustainable approaches to delivering:

Our services include:

Gap analysis and remediation planning

Critical process identification, mapping and resilience assessment

Development of Operational Resilience policies and frameworks

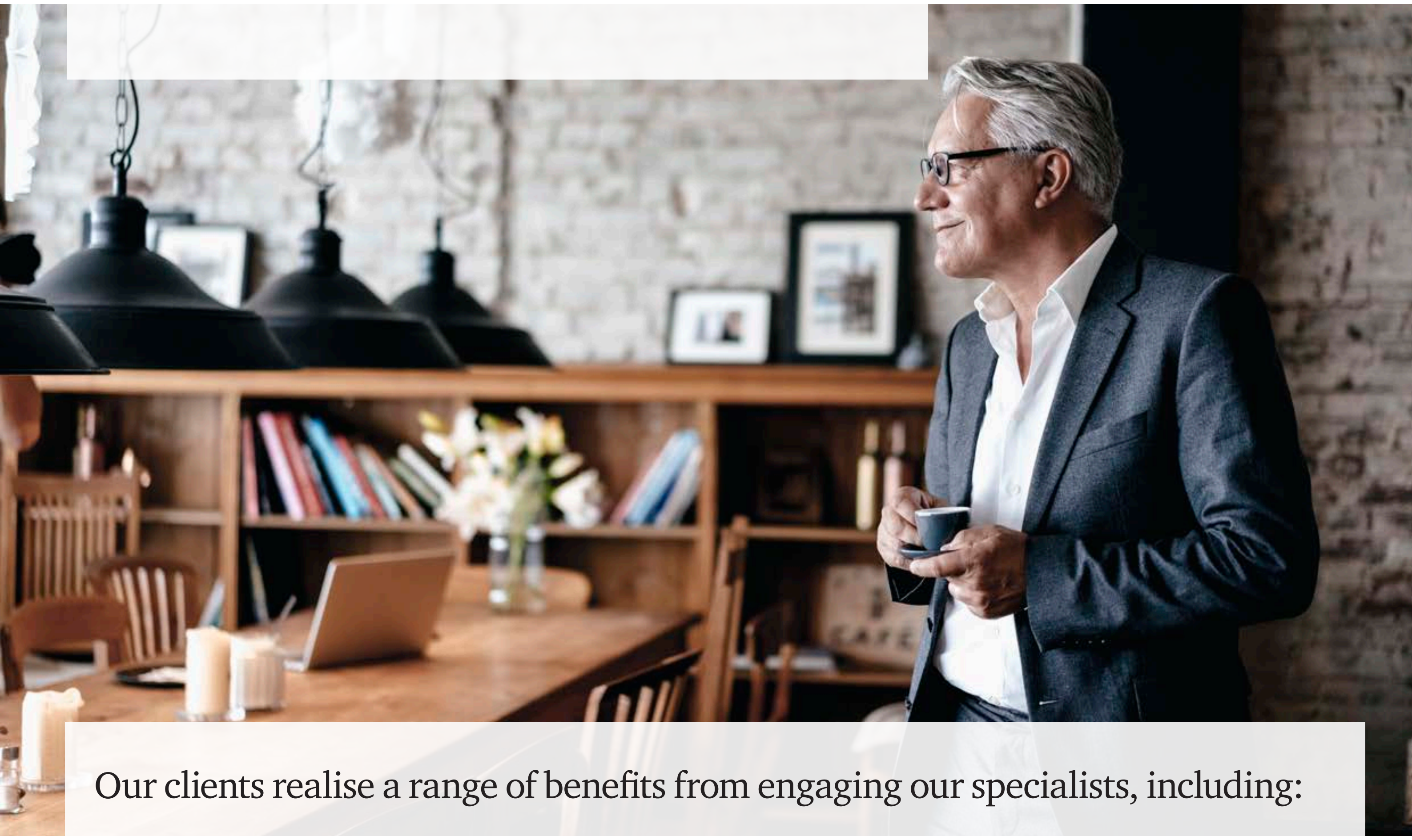
Assessment, remediation and optimisation, including Target Operating Model design, across risk-resilience functions including Enterprise Risk Management, Business Continuity Management, Crisis Management, IT Resilience, Cyber and Security.

Supply Chain resilience

Infrastructure resilience, including technology, IT, real estate, facilities management, and critical assets

People capability, skills analysis and planning

What you gain



Our clients realise a range of benefits from engaging our specialists, including:

1. Increasing stakeholder confidence in your ability to deliver what you promise
2. Taking a risk-balanced approach to Operational Resilience, ensuring effort and investment is focused where it matters most
3. Minimising costs and losses of unacceptable disruption
4. Improved safeguarding of organisational brand/reputation
5. Delivering the resilience programme in a way that captures insights that can also be used to inform strategic decision-making and risk management
6. Ability to respond confidently to regulator and stakeholder requirements for Operational Resilience assurance

When to act

Ultimately, there are a range of common triggers that prompt our clients to seek support. These include:

Here are some of the common triggers:

- *Increased regulatory attention on Operational Resilience*
- *Competitors gaining advantage through enhanced Operational Resilience*
- *Costs associated with potential unreliability, including share price considerations*
- *Increasing operational complexity*
- *Desire to improve reliability and stakeholder comfort levels*
- *Incidents resulting in unacceptable losses*

# Intelligent Digital

At PwC, we are harnessing the power of Intelligent Digital, helping our clients to rethink their futures and reshape their own world. We are using business understanding, innovation in technology and human insight to help solve important problems, meet human needs and make a difference to society.

Helping our clients to understand the bigger picture of where their compliance operations, practices and controls fit into the regulatory landscape, and how they can be streamlined and improved to better safeguard them from risk, lies at the heart of PwC's support in the Compliance function.

Our teams help to build more simple, universal and integrated frameworks that deliver a clear understanding of compliance risk for our partners. Techniques and practices including culture and behavioural assessment, compliance programme remediation and third-party compliance programme development all stem from our commitment to the Intelligent Digital philosophy.

pwc.co.uk/intelligentdigital
#IntelligentDigital

Get in touch

Nicola Shield
Partner, Governance Risk and Compliance, PwC
M: +44 (0)7931 388648
E: nicola.j.shield@pwc.com

Matt Elkington
ERM Practice Leader, PwC
M: + 44 (0)7595 609663
E: matt.elkington@pwc.com

Charley Newnham
Enterprise Resilience Director, PwC
M: +44(0)7930 402575
E: charley.newnham@pwc.com

October 2018

pwc.co.uk

This content is for general information purposes only, and should not be used as a substitute for consultation with professional advisors.

180928-170754-KK-OS