EY's response to ‘Building the UK financial sector’s operational resilience’ – a BoE/FCA/PRA Discussion Paper

Minds made for protecting financial services
When the financial services industry works well, it creates growth, prosperity and peace of mind for hundreds of millions of people. No other industry touches so many lives or shapes so many futures.

At EY Financial Services, we share a single focus – to build a better financial services industry, not just for now, but for the future.

We train and nurture our inclusive teams to develop minds that can protect financial services. Our professionals come together from different backgrounds and walks of life to apply their skills and insights to ask better questions. It’s these better questions that lead to better answers, benefiting our clients, their clients and the wider community. Our minds are made to build a better financial services industry. It’s how we play our part in building a better working world.

ey.com/ukfs
Operational resilience is the ability of an organisation to **prevent, respond to, recover and learn from** operational disruptions to survive and prosper, and not cause harm to customers and the wider market.

The story so far

Following the financial crisis and the focus on restoring financial resilience, the attention of regulators has shifted more prominently towards operational resilience. Incidents such as high profile outages and service disruptions have had a dramatic impact on both retail and business customers, in many cases resulting in mistrust in the financial markets and financial loss.

On top of rising media, political and regulatory attention on incidents and crises, the financial services operating environment is changing swiftly. With firms facing a more complex set of internal pressures (e.g., legacy technology environments, cost and resource pressures) as well as a growing set of external stresses (e.g., technical innovations, changing customer expectations, increased cyber threats and broader operating ‘eco-systems’), it is easy to see why resilience is such a challenge.

Regulatory focus on operational resilience

Firms and regulators alike have made efforts to address and assess operational resilience in recent years, starting with a series of ‘Dear Chairman’ detailed questionnaires, moving to Prudential Regulation Authority (PRA) requirements for resolution planning, Financial Conduct Authority (FCA) ‘deep dives’ and forensic cyber testing (CBEST). Given the risk high profile incidents and events pose to financial market stability and customer welfare, the level of scrutiny and demands are only going to increase.

The joint Bank of England, PRA and FCA Discussion Paper, ‘Building the UK financial sector's operational resilience’ issued in July 2018, pulls together various strands of regulatory attention into a unified and overarching framework. The fact that this is a joint paper underscores the importance that the regulators collectively attribute to operational resilience. Whilst this is a Discussion Paper, it would be reasonable to expect that to a large extent, it outlines the key tenets which these UK regulators expect firms to adopt in the period ahead.

Discussion Paper at a glance

The key requirements noted in the Discussion Paper include:

- **Governance**: the paper has emphasised the importance of operational resilience in the Boardroom. Businesses will be expected to recognise that operational resilience should be high up on their agenda, requiring appropriate executive consideration and oversight. Accountabilities and responsibilities for senior management will need to be clearly defined, set against an unambiguous chain of command.

- **Transparent eco-system**: an organisation’s eco-system must be properly understood, including key business services and the people, systems, processes and third parties that support them, with accountabilities agreed.

- **Risk appetite and tolerances**: organisations will need to understand and clearly articulate their operational risk appetite and impact tolerance for disruptions to key business services, through the lenses of impact to markets, consumers and business viability. The paper adds a systemic ‘overlay’ expecting firms to take into consideration the implications of their interconnectedness with other financial institutions when setting their tolerances for disruption.

- **Planning and communications**: organisations will need to have meaningful plans to prepare for a disruption and ensure that customers, the wider market and regulators are informed of an incident. Heavy emphasis is placed on the performance of these plans with proposals for them to be tested not only by organisations themselves but across their eco-system. There is also a commitment from the regulator to develop a testing programme akin to the long established stress testing model in relation to financial resilience.

- **Culture**: to date, most firms have adopted a ‘fix on fail’ approach to resilience that is focused on processes and operations, rather than the business services that rely on these operations. There must now be a shift in mind-set towards service continuity and a continuous improvement approach, by embedding a ‘resilience culture’ which reinforces and promotes resilient behaviours.

- **Scope**: the themes of the Discussion Paper are applicable to all types of firms and FMIs although it is proposed that the application will differ depending on size, activities and interconnectedness

This sets a new reference for firms, which will become another aspect of the ‘cost of doing business’.
Key challenges for your firm

Operational resilience is not a new topic and firms are likely to already have a number of the components in place, including Business Continuity Planning, Disaster Recovery and Crisis Management. However firms cannot be complacent as this narrow approach is no longer sufficient, as shown by the regulatory requirements for firms to focus more on the topic and raise the bar. It’s clear that a key challenge for firms is the need to integrate these aspects into a holistic approach, breaking down existing organisational and process silos.

From speaking to clients, we see the key challenges in aligning to the Discussion Paper as:

► Establishing clear Senior Managers accountability and responsibility for operational resilience
► Evidencing a customer and market driven approach to the prioritisation of key business services and establishing an internal and external facing approach to defining impact tolerances
► Determining and implementing metrics to monitoring for operational disruption and supporting enhanced decision making at executive levels
► Anticipating and preparing for risks to resilience across the eco-system that firms operate in, recognising that issues in the broader eco-system may have a detrimental effect upon the firm and vice versa
► Building operational resilience into the culture of the organisation and adopting a ‘resilience by design’ mind-set into how the firm designs and operates its strategies, processes and technologies
► Reviewing current talent strategies to ensure access to employees with the necessary resilience skills and experience

Firms must transform how they view operational resilience, and many are already on their way along the improvement journey. A heavy dependence on resilience efforts led by IT is no longer sufficient. A strategic, integrated enterprise-wide resilience program is required, driven by the business and a strong understanding of internal and external connections and dependencies. Continuous review and evolution of the approach is critical to address new resilience risks.

“Today’s Discussion Paper raises the bar in terms of the standards that firms, particularly systemically important organisations, will be expected to meet going forward, and positions it squarely as a Boardroom top priority, alongside financial resilience.”

Ali Kazmi,
Partner, Ernst & Young LLP,
EMEIA FS IT Risk & Resilience Lead

The shape of things to come

The spotlight on operational resilience will continue to increase over time. Regulatory attention is likely to move towards enhanced resilience stress testing standards and refining performance metrics. The Financial Policy Committee (FPC) is establishing its own tolerances for the disruption of financial systems from cyber incidents, which includes a resilience baseline for firms, regular testing and response plans for dealing with attacks. This is an aspect for organisations to consider when setting their individual tolerances. We anticipate regulations extending beyond continuity in resolution to operational and business continuity in normal circumstances.
EY’s response to ‘Building the UK financial sector’s operational resilience’ — a BoE/FCA/PRA Discussion Paper

How EY can help you
Minds made for protecting financial services

EY is ideally placed to support organisations address their operational resilience needs. Our dedicated financial services professionals have experience in business process analysis, technology, infrastructure and cyber risks, crisis management and operational risk. Utilising our proprietary and proven operational resilience frameworks and tools, we can help firms establish and adopt a broad, business lead consideration of operational resilience.

Our work with a broad range of local and global financial services clients on their resilience agenda, including responses to regulatory inquiries, has enabled us to derive insights on what good resilience management looks like.

Our services span areas across the end to end operational resilience processes — identify, map, assess, test, invest and communicate. We are well-positioned to assist firms pre-, during and post-disruption, not only with compliance to the emerging regulations, but to improve overall resilience for business benefit.

Sense, Resist and React to disruptive events, whilst Adapting and Reshaping operations in environments characterised by both foreseeable and unforeseeable risk:

“For firms that do not step up to the mark, they risk reputational and regulatory consequences.”

Ali Kazmi

Contact

Ali Kazmi
Partner
Ernst & Young LLP,
EMEIA FS IT Risk & Resilience Lead
+44 20 7951 9052
akazmi@uk.ey.com

Steve Holt
Partner
Ernst & Young LLP, IT & Cyber Risk
+44 20 7951 7874
sholt2@uk.ey.com

Gareth Lambert
Partner
Ernst & Young LLP, Regulatory Driven Transformation
+44 113 298 2581
glambert@uk.ey.com

Chris Richardson
Partner
Ernst & Young LLP, Operational Risk
+44 20 7951 1012
crichton4@uk.ey.com
About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP
The UK firm Ernst & Young LLP is a limited liability partnership registered in England and Wales with registered number OC300001 and is a member firm of Ernst & Young Global Limited.