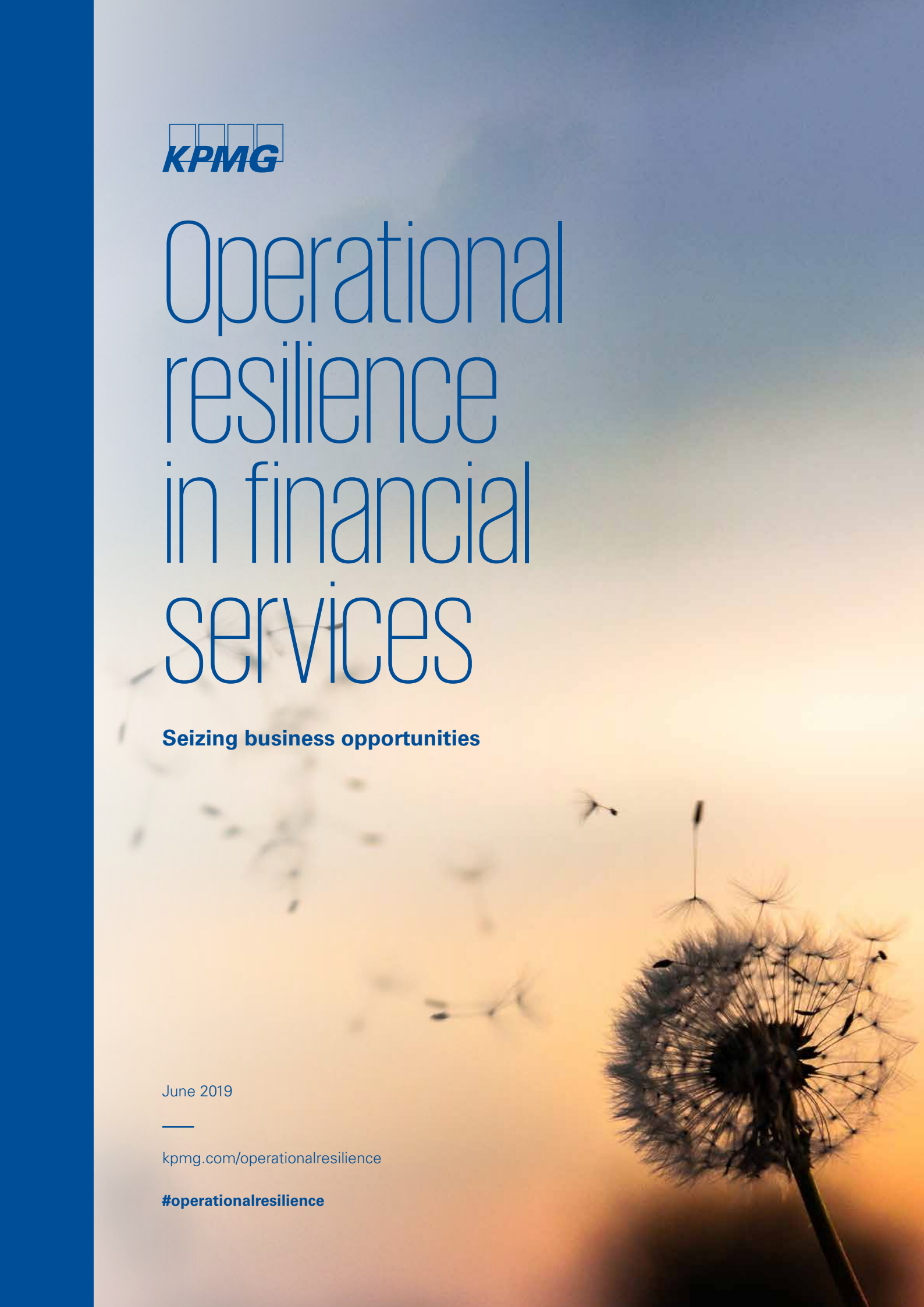


Operational resilience in financial services

Seizing business opportunities

June 2019

kpmg.com/operationalresilience

#operationalresilience

Contents

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

01 Executive summary

Operational resilience is usually defined as the ability of an organisation to adapt rapidly to changing environments. This includes both the resilience of systems and processes and more generally the ability of the organisation to continue to operate its business in the event of disruptive events.

Operational resilience has always been an important area of focus for financial institutions and their regulators and supervisors. However, this focus has sometimes been confined to a narrow set of risks (for example IT security and outsourcing), or to an emphasis on preventing operational disruptions rather than on responding to and recovering from disruptions when they occur.

More recently, the emerging approach of regulators in the UK in particular has taken a broader view of operational resilience, covering all risks to the provision of key business services and focusing increasingly on how the continuity of key business services could be preserved in the event of disruptions occurring. This represents a fundamental shift in how financial institutions in the UK should approach operational resilience.

Although the adoption and application of such a broader view in other countries is likely to be uneven across countries and across sectors, there are clear signs of movement in this direction, which will have implications for financial institutions beyond the UK.

In the EU, US, Australia, Hong Kong and Singapore the range and depth of regulatory requirements relating to various aspects of operational resilience are expanding rapidly, while operational resilience has moved sharply up the supervisory agenda. This includes an increasing focus on the response and recovery of financial institutions to operational disruptions.

There will clearly be costs to firms in meeting these evolving regulatory requirements. But this should not be seen as purely a compliance exercise. There are also opportunities for firms to strengthen their operational resilience in a way that brings business benefits. Taking a more explicit end-to-end view of key business services should enable firms to drive more than operational resilience. It should also enable them to:

- Generate synergies across strategic, financial and operational resilience
- Generate better customer outcomes and enhance customer trust and loyalty
- Reduce their operational risks and the costs of disruption
- Be better positioned for mergers, acquisitions and moves into new areas of business or new ways of doing business
- Allocate resources more effectively and efficiently.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

02 Implications for firms: costs and opportunities

Financial institutions are already subject to a wide range of regulatory requirements and supervisory expectations relating to their operational resilience.

A broader view of operational resilience by regulators and supervisors would however place more emphasis on the ability of firms not only to control their operational risks but also to manage disruptions when they do occur in order to preserve the continuity of key business services.

Firms are already undertaking multiple risk management activities under the broad umbrella of operational resilience. Cyber security and third party risk management are but two of the most prevalent recent examples of such risk management activities that are common across many firms and jurisdictions.

However, to a large extent these risk management activities have taken the form of vertical operational risk frameworks focusing primarily on individual systems and processes, and on reducing the probability or risk of a disruption occurring.

Similarly, although firms also have long experience of business continuity planning and incident management, these have often been somewhat narrowly focused on responding to a limited range of disruptions.

A wider view of operational resilience would augment, rather than duplicate, the existing operational risk management and business continuity planning approach by taking a more horizontal, end-to-end view of the continuity of a firm's key business services.

Responses to regulation

In response to regulators and supervisors taking a broader view of operational resilience firms will need to:

- Embark on a transformative programme, overseen by senior management and the Board, to embed a culture of resilience, shape the firm's strategic agenda and investment decisions from a resilience perspective, identify priority business services, and set impact tolerances
- Establish clear accountability structures for operational resilience, particularly in countries with individual accountability regimes (including Australia, Hong Kong, Singapore and the UK)
- Adapt and develop approaches that go beyond traditional contingency planning, disaster recovery, incident management, operational risk management and third party risk management, to focus through a business lens on managing disruption, whatever the cause, and on delivering the continuity of key business services. Operational resilience should not be treated as just another compliance exercise
- Assume that operational disruptions will occur, and develop coordinated response and recovery mechanisms to such disruptions, including the definition of escalation paths and decision-making procedures, and effective internal and external communication plans which will provide timely information for customers, other market participants and the regulator
- Define recovery plans that enable the resumption of key business services within threshold tolerances when disruptions occur, and use severe but plausible scenarios to conduct end-to-end testing of the firm's operational resilience.

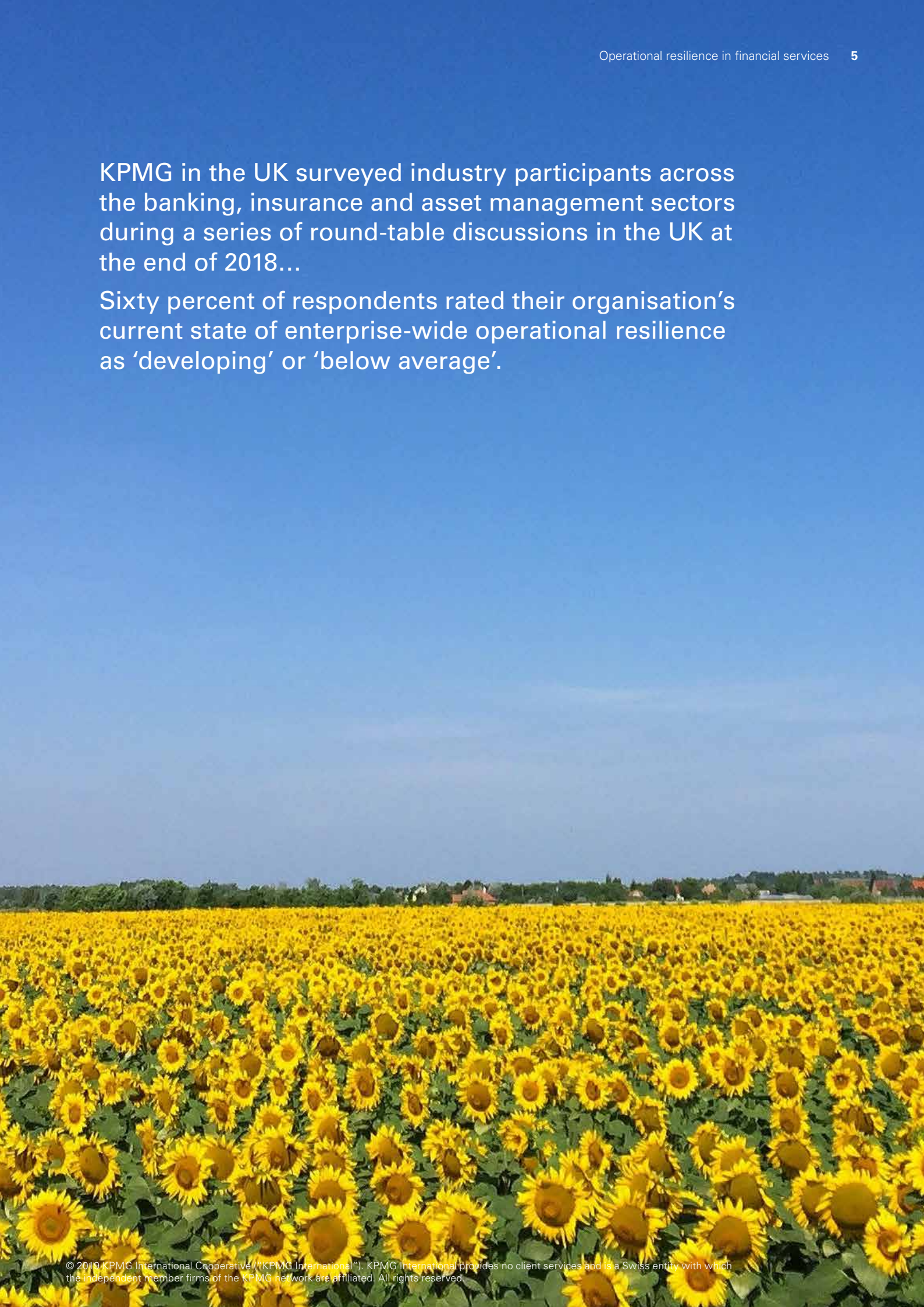
This may require a major shift in approach for many firms.

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

KPMG in the UK surveyed industry participants across the banking, insurance and asset management sectors during a series of round-table discussions in the UK at the end of 2018...

Sixty percent of respondents rated their organisation's current state of enterprise-wide operational resilience as 'developing' or 'below average'.



© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Turning operational resilience into a business opportunity

The evolving regulatory approach to operational resilience could also bring significant benefits to firms.

These benefits – and the costs of meeting regulatory requirements in this area – will depend to a large extent on the ability of firms to drive down costs and to boost efficiency and effectiveness through the more effective leveraging of data, data models and systems architecture. Improved operational resilience often requires convergence, simplification and an end to duplication of regulatory, risk and control frameworks; and rationalising service and process overlaps. Such gains have the potential to enable headcount rationalisation and to unlock a broad range of efficiency savings.

1.

Generate synergies across strategic, financial and operational resilience

At the highest level, a firm's overall enterprise resilience can be divided into strategic resilience (the resilience of the firm's strategy and market position), financial resilience and operational resilience. Elevating operational resilience to equal status to strategic and financial resilience should help firms to align their approach to operational resilience with the firm's strategic goals and to anticipate and navigate both the operational and the financial risks that emerge from increasingly complex and inter-connected business models.

2.

Enhance customer trust and loyalty

Recovering rapidly to deliver good customer outcomes and retaining customer trust and loyalty in increasingly competitive markets should be a key driver of success for firms. Customer trust and loyalty may be enhanced through the ability of a firm to out-perform its competitors in terms of both preventing disruptions from occurring and continuing to deliver its key business services as seamlessly as possible when adverse shocks do occur. The alternative is that firms run the risk that the costs of mitigating and redressing disruptive events may be compounded by the potential damage to reputation and customer confidence and a resulting loss of business.

3.

Reduce operational risks and the costs of disruption

A greater end-to-end focus on business services, and clearer accountabilities based on such a focus, should enable a firm to reduce its operational risks, reduce both the probability of disruption and the impact of disruptions when they do occur, and thereby drive down regulatory capital requirements and the costs of fines and other regulatory sanctions.

4.

Enhance positioning for mergers, acquisitions and moves into new areas of business or new ways of doing business

A clearer understanding and mapping of business services and the people, data, systems and processes on which they depend should enable a firm to undertake mergers and acquisitions more efficiently and effectively, and enable a firm to move more smoothly into new areas of business or new ways of doing business.

5.

Allocate resources more effectively and efficiently

Rebalancing efforts from trying to prevent disruption to focusing more on response and recovery when disruption does occur should enable firms to allocate resources more effectively and efficiently. Basing investment decisions on what is most important to the continuity of key business services, on the results of scenario tests and on whether a service can be recovered within impact tolerance thresholds should reduce costs and contribute to competitive advantage.

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

03 Regulatory approaches to operational resilience

Financial services regulation has typically focused on operational risk rather than on operational resilience in a broader sense. This has emphasised the importance of risk management to reduce the probability of a disruptive event occurring, and has focused primarily on the financial consequences of a failure in people, systems or processes. But this is changing.

Operational resilience is not a new concept for financial institutions. Business continuity planning dates back to the 1970s, cyber-attacks first became prevalent in the 1980s, and concerns about IT security date back as far as the use of IT.

Similarly, both financial institutions and their regulators and supervisors have focused increasingly on the potential risks of disruption to the outsourcing of services to third party suppliers, the privacy and security of data held by financial institutions, and most recently on operational continuity in resolution (in particular for large banks and central clearing counterparties).

Many of these concerns have intensified as financial institutions (and, through them, economies more generally) have become more vulnerable through the opening of digital access routes, the increasing adoption of fintech, the greater use of outsourcing, the widening range of cyber threats and the demands of customers for high quality services. These vulnerabilities have been well illustrated by the increasing number of high profile and high impact incidents which have struck financial institutions across the globe, from cyber-attacks to IT failures.

Overview

Although major countries have taken broadly similar approaches to the regulation and supervision of operational risk, and of operational resilience, more generally, the areas of emphasis and the details of rules and guidance have differed across countries and across sectors.

This reflects in part the absence of agreed international standards, while even where international standard setters have addressed operational resilience this has been through the statement of high level principles. Examples of this include the core principles set out for banks and insurers by the Basel Committee for Banking Supervision and by the International Association of Insurance Supervisors; the Basel Committee's sound practices for operational risk management; the G7's high level fundamental elements for effective cyber security assessment; and the joint guidance from the Committee on Payments and Market Infrastructures and the International Organisation of Securities Commissions on cyber resilience for financial market infrastructures.

Regulatory and supervisory developments on operational resilience in major jurisdictions can be characterised by:

- An increasing emphasis on various aspects of operational resilience
- A piecemeal approach to individual aspects of operational resilience, rather than on operational resilience as an over-arching objective
- An emphasis primarily on system resilience rather than on the continuity of business services – on enhancing the robustness of systems and processes in order to reduce the probability that an operational risk will crystallise, rather than on how a financial institution could respond to and recover from a disruption
- An emphasis on the financial losses to the financial institution arising from an operational failure, rather than on the broader costs and impacts to its customers or to the financial system as a whole.

KPMG

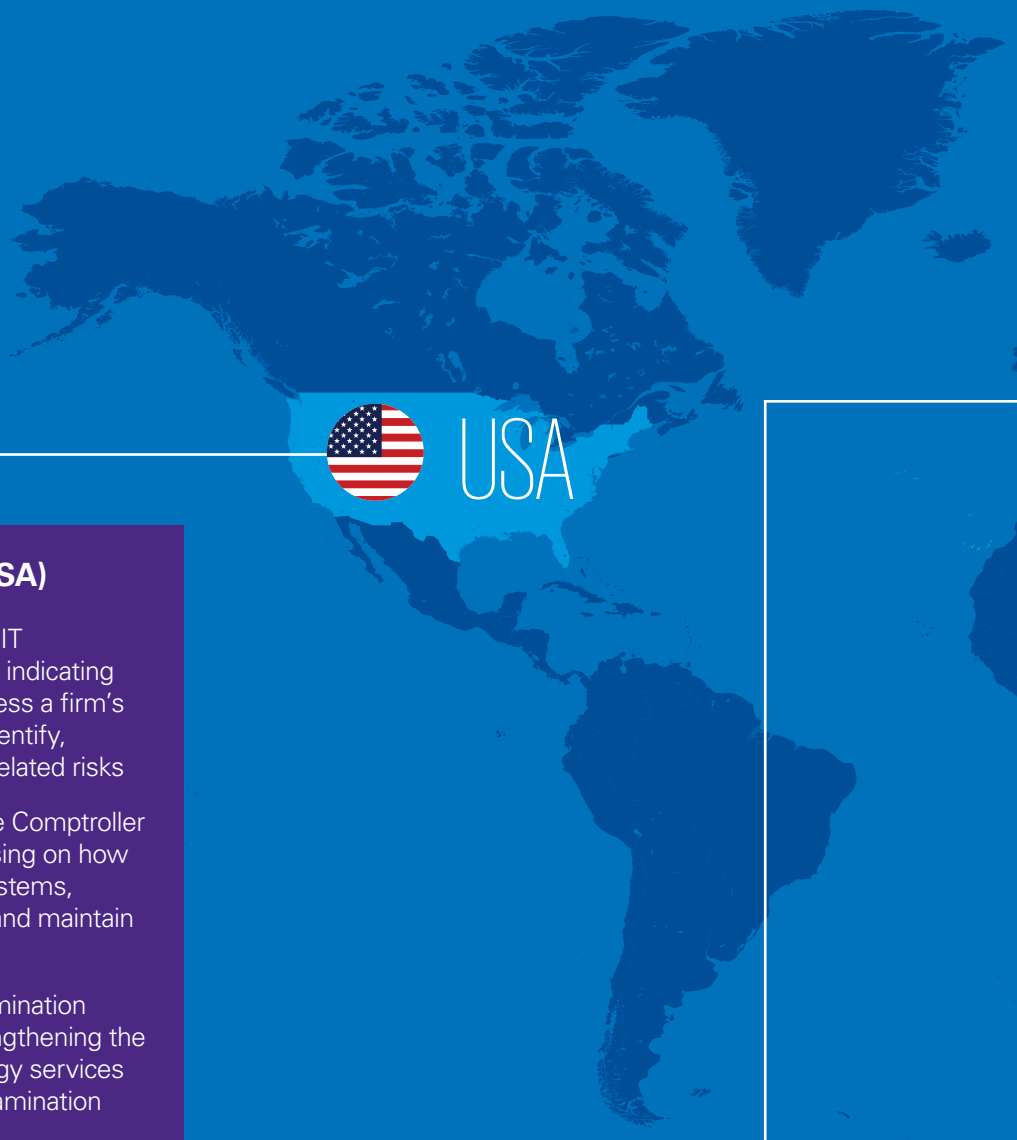
© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

This is not to say that the broader aspects of operational resilience have been ignored. Business continuity planning has always focused in large part on how a business could maintain or resume its services in response to a disruptive event, although this has usually been confined to a relatively narrow range of inputs to a business (premises, telecommunications, data and IT systems). Regulatory standards on operational risk usually mention the response to, and recovery from, operational disruptions – for example with respect to cyber security risks the standard framework runs from prevention to identification and detection and then to response and recovery.

It is also clear that greater supervisory emphasis is being placed in many major countries on response and recovery. The balance of focus is shifting from reducing the probability of disruption to the response and recovery aspects. This trend is more pronounced in the regulation and supervision of the banking sector than for other sectors. However, even in the banking sector this is mostly concentrated on response and recovery in the context of IT systems and cyber security, and does not always extend to the continuity of business services.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Examples of rules and guidance issued by regulators relating to operational resilience



United States of America (USA)

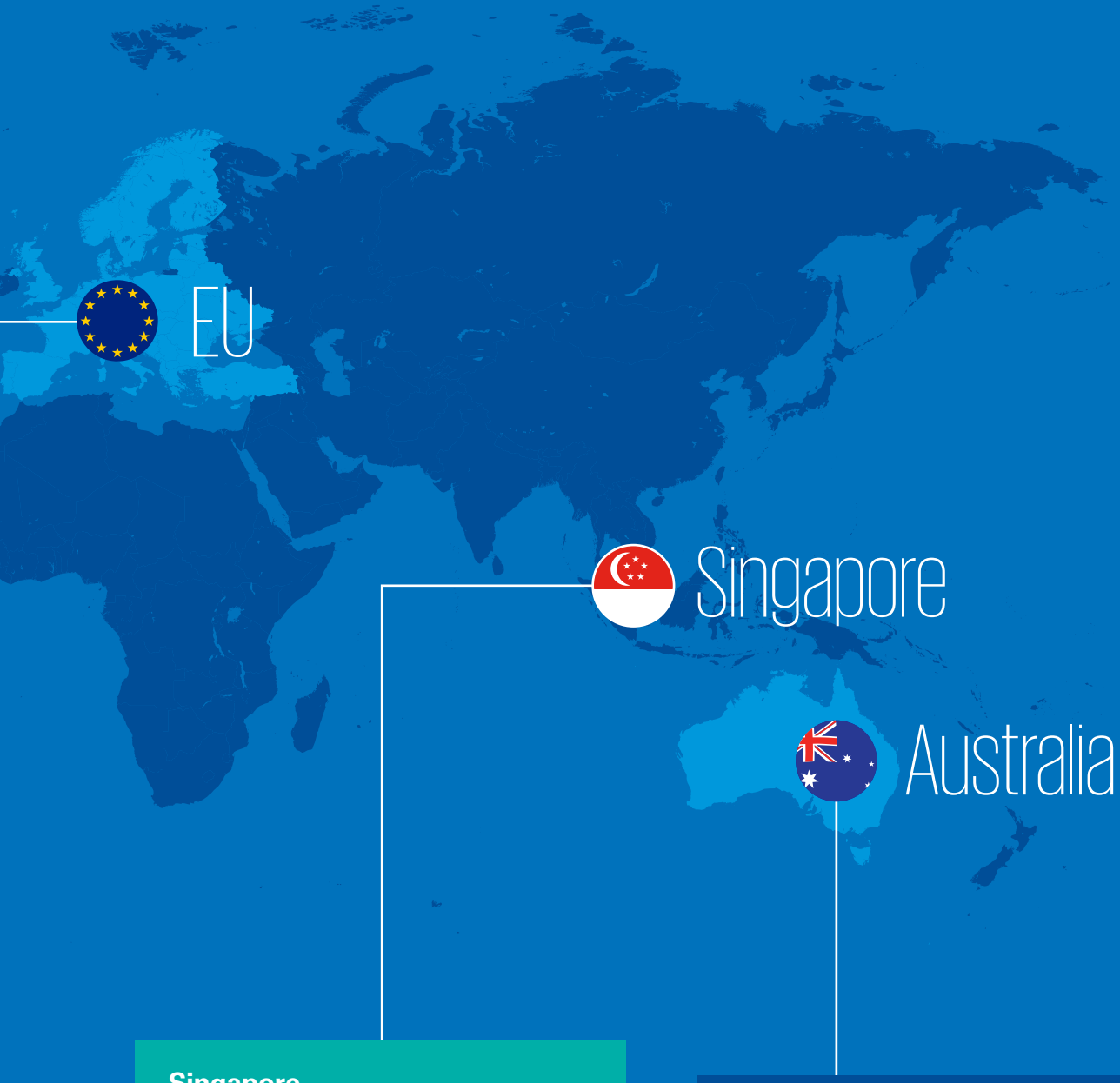
- Federal Reserve guidance on the IT supervisory examination process, indicating how examination staff would assess a firm's risk management processes to identify, measure, monitor and control IT-related risks
- Federal Reserve and Office of the Comptroller of the Currency (OCC) rules focusing on how a firm protects and secures its systems, media and facilities that process and maintain information vital to its operations
- Federal Financial Institutions Examination Council (FFIEC) guidance on strengthening the resilience of outsourced technology services (in Appendix J of the FFIEC IT examination handbook)
- Federal Reserve guidance on business continuity and disaster recovery, including measures to promote the continuous operation of financial markets and to ensure the continuity of operations in the event of a crisis
- Federal Reserve focus on operational deficiencies in its rating system for large financial institutions (LFIs), and on operational resilience in its consolidated supervision framework for LFIs
- Financial Services Sector Coordinating Council guidance on business services resilience and restoration

European Union (EU)

- EBA Guidelines on ICT and security risk management
- ECB Cyber Resilience Oversight Expectations for financial market infrastructures (FMIs)
- TIBER-EU framework, the first European framework for controlled cyber hacking to test the resilience of financial institutions
- EBA Guidelines on outsourcing arrangements

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.



Singapore

– Updating of multiple detailed Monetary Authority of Singapore regulations on cyber security and technology risk, business continuity and outsourcing

Australia

– New or updated APRA standards on operational risk, outsourcing and service provision, business continuity and information security

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

EBA Guidelines on ICT and security risk management

The EBA consulted in December 2018 on draft Guidelines on information and communication technology (ICT) risks and security risk management. The draft Guidelines set out requirements for credit institutions, investment firms and payment service providers (PSPs) on the mitigation and management of their ICT risks.

EBA notes that firms' reliance on ICT makes them increasingly vulnerable to ICT failures, from internal and external attacks (including cyber-attacks); from system outages; and from inadequate business continuity planning for ICT systems and processes, or poor processes relating to ICT change management.

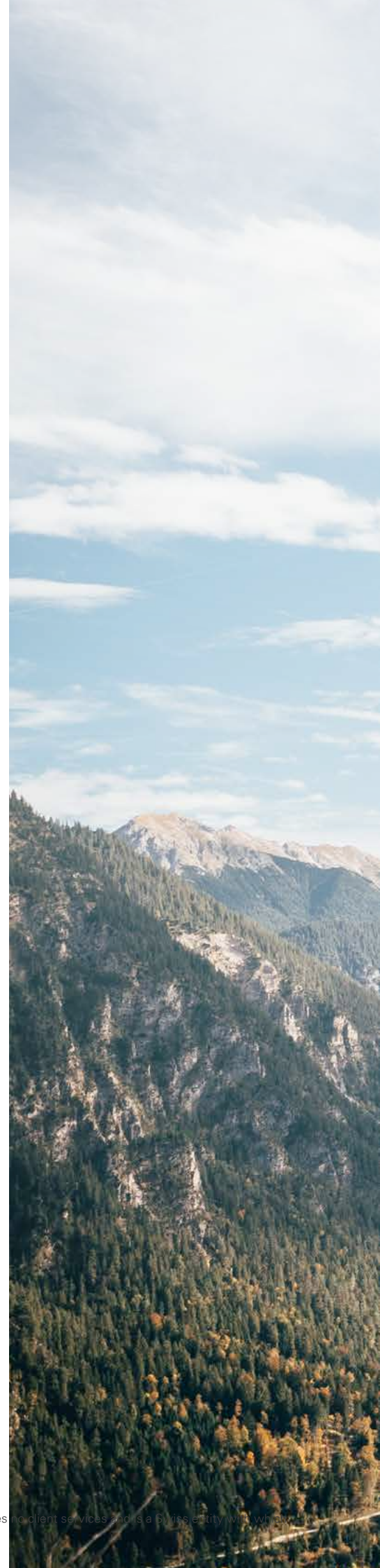
Firms therefore need to put in place the governance, risk management frameworks and information security procedures and processes to reduce the risk of ICT failures and to enhance their ability to recover and respond if such failures do occur. The draft Guidelines include a long list of detailed requirements on firms, clarifying the regulatory requirements on ICT and security risk management and aligning these with the supervisory assessment of firms' ICT risks.

The draft Guidelines cover the mitigation of ICT and security risks through a firm's:

- Governance
- Risk management framework and assessment process
- Information security policy, requirements, monitoring, testing, training and review
- ICT operational management
- Treatment of ICT in change and development processes
- Business continuity management.

The draft Guidelines also highlight some specific characteristics of cyber security that firms should take into account in ensuring that their information security measures are adequate:

- Unlike most other sources of risk, malicious cyber-attacks are often difficult to identify or fully eradicate and the breadth of damage can be difficult to determine
- Some cyber-attacks can render common risk management and business continuity arrangements ineffective and they might in some instances fuel the propagation of malware and corrupted data to backup systems
- Third party service providers, vendors and vendors' products may become a channel to propagate cyber-attacks.



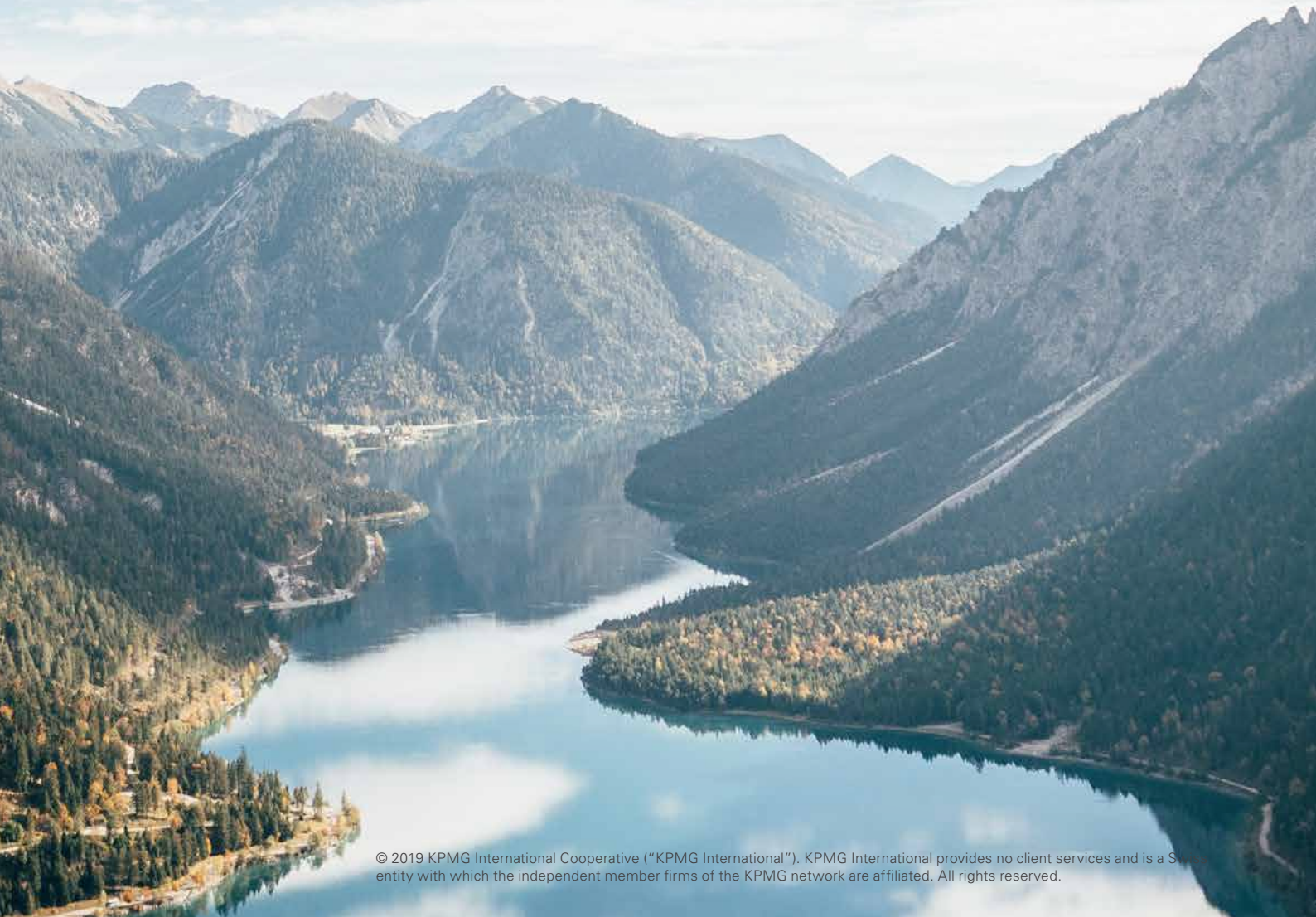
KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

APRA standards on business continuity

The Australian Prudential Regulation Authority (APRA) updated its prudential standards on business continuity management in July 2017. These require APRA-regulated institutions to:

- Identify, assess, manage, mitigate and report on potential business continuity risks to ensure that the institution is able to meet its financial and service obligations to its depositors, policyholders and other stakeholders
- Ensure that business continuity risks and controls are taken into account as part of the institution's risk management strategy
- Take a whole-of-business approach that includes policies, standards and procedures for ensuring that critical business operations can be maintained or recovered in a timely fashion in the event of a disruption, and thereby minimise the financial, legal, regulatory, reputational and other material consequences arising from a disruption
- Consider plausible disruption scenarios over varying periods of time, the period of time for which the institution could not operate without each of its critical business operations, the extent to which a disruption to the critical business operations might have a material impact on the interests of depositors and/or policyholders of the institution, and the financial, legal, regulatory and reputational impact of a disruption to the institution's critical business operations over varying periods of time
- Set pre-defined goals for recovering critical business operations to a specified level of service (recovery level) within a defined period (recovery time) following a disruption.



© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Supervision

The intensity of supervision is also clearly increasing on many aspects of operational resilience, again with some differences in approach and areas of focus across countries and sectors.

USA

In the US, operational resilience is a top priority for the financial services regulators. The Federal Reserve and the OCC undertook a series of examinations in this area for the largest banks last year and plan to continue this focus in 2019, with an emphasis on end-to-end testing and management reporting. New requirements are likely to emerge in the near term, in part from bank examinations.

The OCC's Supervision Plan for 2019 included cyber security and operational resilience in the context of cyber security as a key focus area, with an emphasis on maintaining IT systems and remediating identified concerns, including:

- Regulated firms' ability to keep pace with changing risk environments and regulatory developments
- The internal controls and end-to-end processes necessary for product and service delivery
- The implementation of new or revised products or strategic partnerships
- A heightened focus on control functions and, as appropriate, alignment with existing risk management processes.

The Federal Reserve listed operational resilience as an area for horizontal examination in its 2019 plan. Supervisors will be focusing in particular on:

- The development and implementation of a forward-looking strategy to better understand and address the impact of critical system failures on key businesses, counterparties and the economy
- The depth of understanding of key systems in place to support critical business functions and activities
- The effectiveness of solutions and controls to detect and mitigate threats in the face of increasingly sophisticated technologies and new threats
- The demonstration of appropriate solutions to ring-fence critical aspects of IT systems, including access security.

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

EU

The ECB has been very active as a supervisor in the area of IT security management, primarily through its on-site inspections and its IT Questionnaire, with a strong focus on:

- Information security policies and procedures
- Security reviews
- IT security awareness
- Physical security
- Identity and access management
- Patch and vulnerability management
- Network security (including remote access)
- Security event logging and monitoring
- Malware prevention
- Data classification.

On cyber security, the overall message conveyed by the ECB is that cyber risks need to be seen as part of general risk management procedures, crisis management and business continuity planning. Banks are strongly encouraged by the ECB to cooperate with a wide range of stakeholders (both internal and external) to address cyber risks.

The ECB's supervisory priorities for 2019 include a continued focus on IT and cyber risks, together with an additional focus on IT incident and problem management, and on cloud computing outsourcing.

Australia

In Australia, APRA has recently increased its supervisory focus on institutions' business continuity, disaster recovery and crisis management arrangements. APRA has required regulated institutions to demonstrate and report on how they would respond to multiple and cluster outage scenarios and data centre failures, and to complete data recovery tests.

Institutions' business continuity arrangements should cover a consideration of acceptable outage periods relative to actual recovery timeframes, the application of a methodology for the 'tiering' of business process criticalities (with specific tolerances defined for outages across these critical processes), impact assessment reviews as part of IT enhancement programs, and reconciling IT and business impact assessments, including recovery testing.

Hong Kong

In Hong Kong, in addition to major initiatives on cyber security testing, the HKMA has conducted on-site examinations focusing on regulated institutions' cyber security controls, outsourcing arrangements and IT governance. In 2018, 23 percent of on-site examinations and thematic reviews covered IT and operational risk management.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

04 Emerging UK approach to operational resilience

A joint Discussion Paper from the Bank of England, PRA and FCA in July 2018 signalled a shift in approach to the regulation and supervision of operational resilience in the UK. The proposed approach emphasises the desired outcome of the continuity of key business services, the importance of financial institutions' responses to and recovery from disruptive events, and the implications of this for governance and individual accountability.

The UK joint Discussion Paper defines operational resilience as "the ability of firms, financial market infrastructures and the financial sector as a whole to prevent, respond to, recover and learn from operational disruptions". This makes it clear that the focus of the proposed approach is not just about operational risk and risk control - the "prevent" part of the equation in seeking to reduce the probability of a disruptive event occurring - but also about minimising the impact should a disruptive event occur.

It is also clear that the UK authorities are looking to pull together all the various elements of operational resilience into a single location – as is evident from the statement in the PRA's latest business plan that the PRA wants to see the world in terms of financial resilience and operational resilience.

Similarly the FCA wants to pull together the risks to consumer harm from insufficient operational resilience and the Bank of England wants to monitor the implications for financial stability from system-wide disruption, common vulnerabilities (for example financial institutions relying on common third parties) and the adequacy of resources collectively.

This represents a fundamental shift in how financial services firms should approach operational resilience.

The PRA and FCA plan to issue consultation papers later in 2019 setting out their approaches in more detail.

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

UK emerging approach to operational resilience: expectations on financial institutions

1. Board leadership

- Take a top-down integrated view of operational resilience, led and driven by the board and senior management
- Boards and senior management will need to ensure that they have sufficient expertise and information on operational resilience, and that they establish enterprise-wide operational resilience procedures with appropriate staff and budget
- Identify under the UK's Senior Managers Regime which senior manager(s) are responsible and accountable for operational resilience.

2. Operational resilience culture

- Embed a resilience culture and use operational resilience considerations to drive investment decisions.

3. End-to-end business service approach

- Continue to focus on the "prevent" aspects of operational risk management - avoiding disruption to systems or processes contributes to operational resilience but is not enough in itself
- Establish and manage operational resilience across key business services, and focus on business service continuity as an outcome for the end-customer, rather than solely on a collection of disparate systems and other inputs
- Identify the people, data, systems and processes that support key business services, and map these services across functions and entities, including external suppliers.

4. Specify tolerances

- Establish impact tolerances (using specific outcomes or metrics) from a consumer, business and financial stability perspective, for example for the length of time that a key business service could be unavailable
- Prioritise efforts on those services that if disrupted may cause customer harm, imperil the viability of the firm, or undermine financial stability.

5. Testing

- Establish rigorous end-to-end testing programmes which challenge the firm's ability to remain within tolerances in severe but plausible scenarios, and which identify the interactions and interdependencies required to deliver services.

6. Recovery and response

- Assume that disruptive events will occur so that the focus is on planning for what happens when a disruption occurs
- Focus on responses to a disruptive event, such as the ability to identify rapidly the scale of the impact
- Focus on the ability to recover from a disruptive event, through robust and well-tested (through severe but plausible scenarios) recovery plans based on adaptability or substitutability to enable the continuity or resumption of key business services within agreed tolerances.

7. Effective communication

- Communicate effectively internally, including upward reporting and effective decision-making, and externally with those affected (customers, other financial institutions) and other stakeholders to manage expectations and restore confidence.

8. Continuous improvement

- Take action where necessary to improve prevention, response or recovery capabilities.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Will other countries follow the UK?

It remains to be seen to what extent other countries will follow the UK's emerging approach. The UK's approach should have some attractions to regulators in other countries, and indeed to financial institutions:

- It pulls together various strands of operational resilience and places operational resilience on an equal footing to financial resilience
- It is principles-based and does not add a plethora of new requirements to the existing individual elements of operational resilience. The UK regulators would prefer not to be overly-prescriptive in setting out how firms should deliver operational resilience, and will leave it to firms in the first instance to identify their key business services and to establish recovery tolerances
- It places the responsibility and accountability for operational resilience with the board and senior management of financial institutions, alongside the UK's developing individual accountability regime
- The focus on the continuity of key business services provides a framework – but not a detailed 'one size fits all' model – that can apply equally across sectors and across regulators and supervisors with responsibility for prudential, conduct of business (retail and wholesale) and financial stability outcomes
- The focus on recovery and response to operational disruptions provides a framework within which the existing scattered references to recovery and response in existing operational risk rules and guidelines could be consolidated and given greater prominence. It also has a neat parallel to the growing emphasis on firms' recovery planning for shocks to their solvency and liquidity positions
- There is also a parallel here with the supervisory review of firms' own solvency and liquidity assessments – supervisors will have their own views on the recovery tolerances that firms should be seeking to meet, and of the quality of firms' recovery and response plans

There are some signs that the UK's emerging approach may be echoed by international standard-setters. The Basel Committee on Banking Supervision has set up a new Operational Resilience Working Group which will be developing policy in this area. It has focused initially on cyber security, and published a survey of cyber security resilience practices across jurisdictions in December 2018. It may also lead in due course to the Basel Committee issuing principles on operational resilience that go beyond its earlier sound practices for operational risk management.

Meanwhile, the Financial Stability Board's work on cyber security is moving on from its earlier focus on a stocktake of publicly available regulations, guidance and supervisory practices on cyber security in the financial sector and on its Cyber Lexicon, to beginning work on developing a toolkit of effective practices relating to a financial institution's response to, and recovery from, a cyber incident.

Other countries (and the ECB) are more likely to follow the UK's emerging approach once international standards have moved in this direction.

Firms will therefore have to continue for now to meet a patchwork of evolving regulatory requirements and supervisory expectations across jurisdictions. International financial institutions should nevertheless also consider adopting a consistent approach to operational resilience across the whole group. Applying the highest bar of jurisdictional regulation has the benefits of adopting a good practice approach to embed operational resilience across the group, allowing for consistency across processes and systems that span multiple jurisdictions, and pre-empting the likelihood that at some point other jurisdictions will follow suit.

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

05 How KPMG can help

KPMG member firms have established teams of specialists able to support financial institutions on operational resilience.

KPMG professionals can assist with establishing and making operational resilience part of an organisation's culture, including:

Effective governance

- Definition of an operational resilience strategy
- Governance policy established by the board and aligned to the firm's risk management framework
- Setting the tone from the top through an enterprise-wide risk appetite for operational resilience
- Awareness of national and global regulatory and supervisory developments

Building an operational resilience culture

- Clear understanding of operational resilience
- Tone from the top
- Change leadership
- Role of operational resilience culture in decision-making

Service Management Framework definition

- Service management framework design, governance and management
- Key business service definition

Mapping people, data, systems and processes to key business services

- Support robust end-to-end service resilience assessments and reporting
- Map interlinkages and dependencies between systems maintained by different entities
- Map interconnectedness across key business services
- Leverage of existing capabilities
- Knowledge of which systems and processes are capable of being substituted during disruption, and how they can be substituted
- Support business continuity planning and incident management

Tolerances

- Establish impact tolerances for key business services
- Scenario development and testing
- Remedial actions

KPMG

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Recovery and response

- Specification and testing of recovery options
- Decision-making processes
- Communication strategy for internal and external stakeholders

End-to-end testing of operational resilience

- Risk based approach to developing a testing plan
- Identification of the severe but plausible scenarios for testing
- Identification of the testing approach for each service and scenario
- Execution of test to assess operational resilience

Operational resilience management reporting

- Identification and capture of data and information required to be presented in management reporting
- Levels of reporting across services, legal entities and geographies

Target operating model

- Governance
- Organisation, accountability and ownership across end-to-end services
- Processes
- Combine resilience of individual systems and processes with business service level resilience
- Data modelling and management information reporting - dashboards, testing scenarios and tolerance assessments
- Linkages to existing functions/processes including business continuity and incident management
- Business case definition for operational resilience beyond compliance and unlocking a broader set of transformational benefits.

© 2019 KPMG International Cooperative ("KPMG International"). KPMG International provides no client services and is a Swiss entity with which the independent member firms of the KPMG network are affiliated. All rights reserved.

Contacts

Andrew Husband
Head of Operational Resilience and Banking Lead
KPMG in the UK

E: andrew.husband@kpmg.co.uk

Mike Walters
Head of Regulatory Driven Transformation
KPMG in the UK

E: mike.walters@kpmg.co.uk

David Miller
Partner, Insurance
KPMG in the UK

E: david.miller@kpmg,.co.uk

Clive Briault
Senior Advisor
KPMG in the UK

E: clive.briault@kpmg.co.uk

Bill Packman
Partner, Wealth and Asset Management
KPMG in the UK

E: bill.packman@kpmg.co.uk

James Lewis
Head of Risk & Regulatory Insight Centre
KPMG in the UK

E: james.lewis@kpmg.co.uk

Bia Bedri
Head of Cyber - Financial Services
KPMG in the UK

E: bedria.bedri@KPMG.co.uk

kpmg.com/operationalresilience

#operationalresilience

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation. Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

© 2019 KPMG International Cooperative ("KPMG International"), a Swiss entity. Member firms of the KPMG network of independent firms are affiliated with KPMG International. KPMG International provides no client services. No member firm has any authority to obligate or bind KPMG International or any other member firm vis-à-vis third parties, nor does KPMG International have any such authority to obligate or bind any member firm. All rights reserved. The KPMG name and logo are registered trademarks or trademarks of KPMG International.

CREATE. | CRT115014 | June 2019