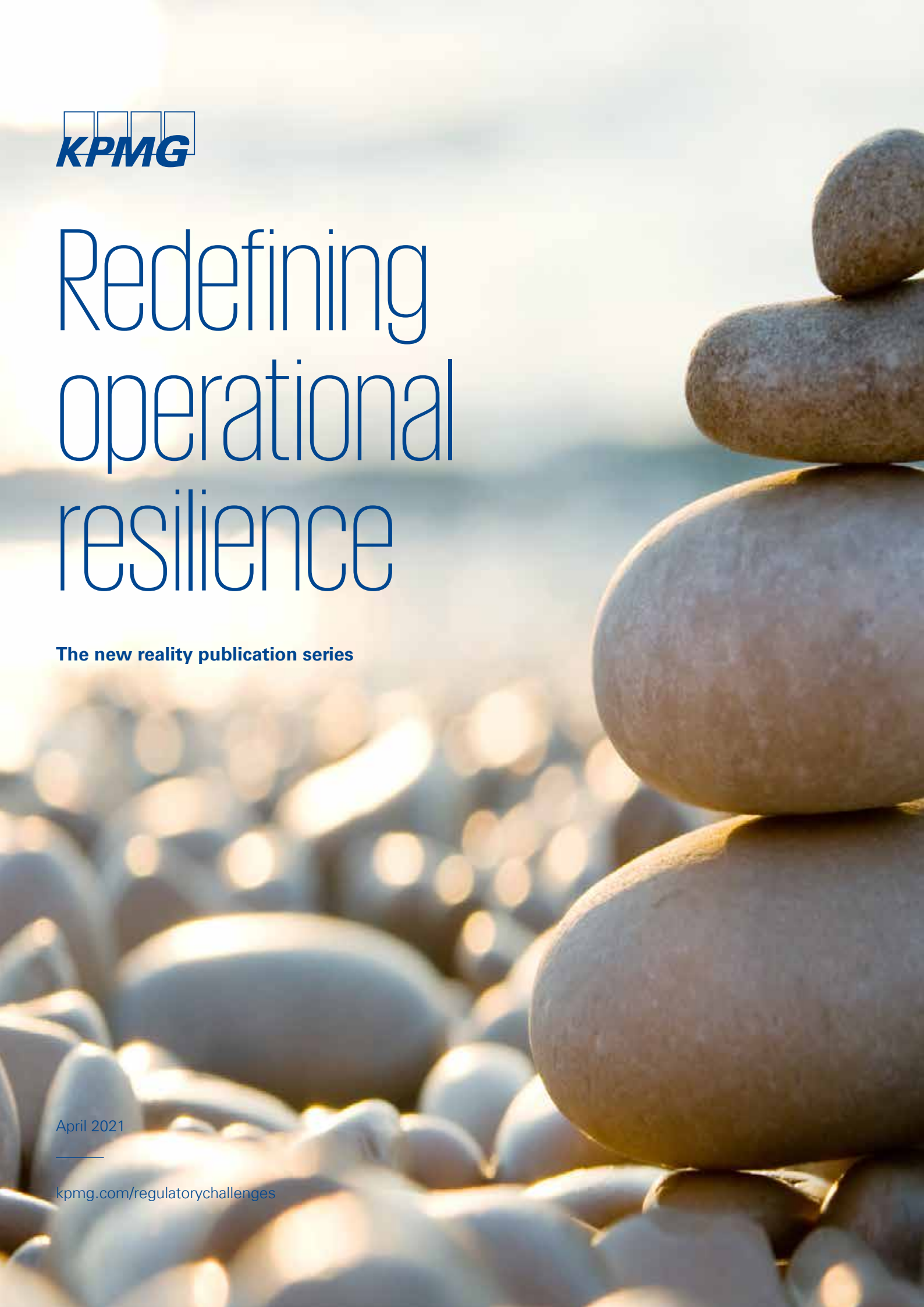


Redefining operational resilience

The new reality publication series

April 2021

kpmg.com/regulatorychallenges

New publication series

The EMA FS Regulatory Insight Centre (RIC) is pleased to publish the seventh paper in its new thought leadership series ***Financial Services: regulating the new reality.***

As the focus of government and businesses moves from initial response to the pandemic, through resilience concerns, to recovery and the new reality, financial services regulators are moving into a new phase of adjustment and support.

In this paper we consider how regulatory perspectives on operational resilience are developing, how the landscape has shifted as a result of COVID-19 and what financial services firms can do now to strengthen their operational resilience through the recovery and beyond. We review the points of agreement and divergence of the emerging regulatory approaches and what these might mean for the forward regulatory agenda for operational resilience.

Look out for the final paper in this series on the evolving regulatory approach to retail conduct issues.

Financial services: regulating the new reality

Remote governance and controls

Delivering sustainable finance

Ensuring stable capital markets

Financial resilience in banking: a balancing act

Accelerating digital finance

Contents

Introduction

Operational resilience has been a regulatory concern for decades but in the aftermath of the 2008 financial crisis it took a back seat to the development of new rules and frameworks for financial resilience. Over the last few years, however, operational resilience has risen to the top of the regulatory agenda and has now been brought into even sharper focus by the COVID-19 pandemic.

Regulators are acutely aware that the threat of disruption to financial firms, and by extension to their customers, is heightened in times of stress. Technology-led business transformation, high-profile instances of disruption and recognition of the interconnectedness of the financial system have led to increased attention on operations and how things are done.

As we move forward into the new reality, financial regulators view operational resilience for banks and insurers on an **equal footing with, and as a key driver of, financial resilience** and recognise that poor resilience has the potential to impact not only individual firms and wider financial stability, but also to cause significant customer detriment. For fiduciary businesses, deficiencies in operational resilience have potential implications for investor returns and security of client assets.

There has been a tangible shift in perspective. Regulators are taking a new approach to resilience: **not if, but when**. They now expect firms to consider not only what would happen if they were to experience disruption, but how they will respond when it does. And although firms were always expected to manage their operational risk, plan for contingencies and have business continuity and disaster recovery plans, in the new reality operational resilience is much more.

Historically, the primary resilience focus for global regulators was cyber and ICT[1] security. These remain critical, particularly under the current stresses of the COVID-19 pandemic, with accelerated adoption of technology and increasing sophistication of external bad actors. Firms must consider the possibility of **multiple concurrent disruptions** and the **emergence of new threats and vulnerabilities**. Extreme events arising from climate change, from floods to wildfires to unexpected snowstorms, could impact physical operations. Geopolitical events could challenge operating models, for example through the loss of operating licences in certain jurisdictions. And evolving business models due to innovation or changes in economic conditions could lead to skill shortages.

Regulatory authorities have realised that a **broader approach** to operational resilience — incorporating equally important components such as people, processes, technology and information — is needed. Customer impact is always in mind and governance and accountability are in the spotlight. Proposed regulations highlight the importance of identifying severe but plausible tailored scenarios, and of performing stress-tests to reveal weaknesses in operating models. Firms are required to define the amount of disruption that they would be willing to tolerate and to monitor and measure their ability to remain within these tolerances.

> "The operational resilience … of financial entities and of our financial system as a whole is just as important as their financial resilience."
>
> **Fabio Panetta**,
> Member of the Executive Board of the ECB

1 Information and Communications Technology

Operational resilience – a regulatory imperative

Operational resilience becomes a **key driver of investment and business strategy**. Firms must have a clear understanding of their end-to-end processes, including critical dependencies, and how these would be impacted by disruption. Increased operational resilience should lead to greater trust amongst all stakeholders including regulators, customers, employees and third parties.

Connectivity is key. The financial services sector in the twenty first century is more interconnected and technology-driven than ever before. Outsourcing has been on the radar for some time, but never on the scale seen now as firms seek to manage down costs and create efficiencies through greater reliance on third parties. Regulators recognise the dominance of a small number of large global technology and infrastructure providers and are seeking to update and expand requirements accordingly.

The **regulatory perimeter is expanding**, with non-financial firms increasingly providing essential services to the financial sector. Operational resilience now means end-to-end resilience throughout the supply chain and this brings many new challenges. The resilience of, and risks associated with, third parties are firmly in the regulators' sights. And as technology and digitalisation continue to gain ground, a broader definition of digital operational resilience is emerging.

For more on COVID-19 as a catalyst for the rapid adoption of technology and its implications for the regulation of financial services, **see our New Reality series paper "Accelerating digital finance"**.

Questions for firms

- How does operational resilience support our business growth agenda and customer strategy? How can it drive improved performance?
- Is operational resilience viewed as a business priority and integral to our business strategy?
- Do we have effective engagement at Board level, and have we assigned clear responsibilities across the firm?
- Have we identified and documented our key/critical/important business services from the perspectives of our own firm, our potential impacts on our customers and, our potential impacts on the wider financial system?
- Do we have end-to-end transparency of services, including third-party relationships?
- Are we confident that our third-party relationships are well-managed and that the contracts we have in place support resilient responses? What are we doing to gain assurance around this? Where contracts fall short, what actions can/will we take?
- Do we have appropriate resources to address capacity and capability risks? Is more and/or specialised resource required?
- Do we have a robust communication strategy for our customers and other key stakeholders?

01. Towards a more holistic approach

The regulatory landscape for operational resilience has evolved over decades and remains fragmented across geographies and sectors. Different jurisdictions are moving at different speeds, but all agree that operational resilience is a priority. Cyber resilience frameworks are well embedded but require monitoring and updating to keep pace with sophisticated threats (see Chapter 3). As definitions of operational resilience grow broader and more complex, regulators are taking different approaches, from high level principles overlaying existing operational risk requirements to the introduction of new operational resilience frameworks.

The UK regulators were widely seen as setting the pace with their coordinated package[2] of consultations for banks, insurers, large asset managers and financial market infrastructures (FMIs) in December 2019, which built on concepts set out in a July 2018 Discussion Paper. The Basel Committee for Banking Supervision (BCBS) is also targeting a holistic approach through its principles for operational resilience, revised in March 2021. The two approaches are intended to be fully compatible but whilst the BCBS principles provide a generic framework, the UK offers a more detailed expression.

Global principles for banks

The BCBS Principles for Operational Resilience[3] build on existing operational risk principles and guidance on corporate governance, outsourcing and business continuity. BCBS also refreshed its Principles for the Sound Management of Operational Risk[4] to address areas where banks were found to need additional guidance in order to facilitate implementation.

The main objective of the principles is that banks should seek to achieve operational resilience by maintaining their ability to "deliver critical operations through disruption". This should enable banks to identify and protect themselves from threats and potential failures and respond and adapt to, as well as recover and learn from, disruptive events. The definition of critical operations is the same as that used in Recovery and Resolution Planning as set out by the Financial Stability Board (FSB) (see Chapter 4). When assessing its operational resilience, a bank should look at its overall risk appetite, risk capacity and risk profile. Operational resilience should be achieved by "harmonising" existing management frameworks and aligning them with the main objective.

Operational resilience is considered as an outcome that benefits from the effective management of operational risk. BCBS expects that banks will be able to incorporate these principles through existing risk frameworks, taking into consideration overall risk appetite, risk capacity and risk profile. It does not suggest a separate framework for resilience.

The BCBS principles are of interest not only to the banking sector but more broadly as a potential blueprint for a global approach. The International Organisation of Securities Commissions (IOSCO) has focused separately on cyber and outsourcing (see Chapters 2 and 3). The International Association of Insurance Supervisors (IAIS) has not specifically addressed operational resilience, although it references limited substitutability, crisis response and management and interruption to

2 https://www.fca.org.uk/news/press-releases/building-operational-resilience-impact-tolerances-important-business-services

3 https://www.bis.org/bcbs/publ/d516.pdf

4 https://www.bis.org/bcbs/publ/d515.pdf

BCBS: High level principles for banks' operational resilience

1. Governance – banks should utilise their existing governance structure to establish, oversee and implement an effective operational resilience approach that enables them to respond and adapt to, as well as recover and learn from, disruptive events in order to minimise their impact on delivering critical operations through disruption.

2. Operational risk management – banks should leverage their respective functions for the management of operational risk to identify external and internal threats and potential failures in people, processes and systems on an ongoing basis, promptly assess the vulnerabilities of critical operations and manage the resulting risks in accordance with their operational resilience approach.

3. Business continuity planning and testing – banks should have business continuity plans in place and conduct business continuity exercises under a range of severe but plausible scenarios in order to test their ability to deliver critical operations through disruption.

4. Mapping interconnections and interdependencies – once a bank has identified its critical operations, it should map the relevant internal and external interconnections and interdependencies that are necessary for the delivery of critical operations consistent with its approach to operational resilience.

5. Third-party dependency management – banks should manage their dependencies on relationships, including those of, but not limited to, third parties or intragroup entities, for the delivery of critical operations.

6. Incident management – banks should develop and implement response and recovery plans to manage incidents that could disrupt the delivery of critical operations, in line with their risk appetite and tolerance for disruption. Banks should continuously improve their incident response and recovery plans by incorporating the lessons learned from previous incidents.

7. ICT including cyber security – banks should ensure resilient ICT including cyber security that is subject to protection, detection, response and recovery programmes that are regularly tested, incorporate appropriate situational awareness and convey relevant timely information for risk management and decision-making processes to fully support and facilitate the delivery of the bank's critical operations.

services in its Holistic Framework[5] for Systemic Risk. The BCBS principles are high-level and sensible and in the absence of other guidance, and notwithstanding sector specific requirements, they could be used by non-bank firms to guide and shape their thinking.

An operational resilience framework for all firms

The UK regulators define operational resilience as: "the ability of firms, FMIs and the sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions". The 2019 consultations set out expectations relating to impact tolerances for important business services[6], and outsourcing and third-party risk management[7]. The UK approach seeks to "prioritise the things that matter" and "drive change where it is needed". The key requirements are:

- **Governance**: operational resilience must be driven from the Board with clear accountability for differentiated investment decisions that properly consider resilience. Accountability is likely to rest with the Chief Operations Function role under the Senior Managers and Certification Regime.
- **Important business services**: Boards and senior management should prioritise resilience for "important business services" – those services that, if disrupted, would pose a risk to the stability of the UK financial sector, a firm's safety and soundness, or the appropriate degree of policyholder protection (for insurers). For many firms, this will mean a shift away from thinking about the resilience of individual systems and resources and a shift towards considering the services that are provided to customers or policyholders.
- **Impact tolerances**: the maximum tolerable level of disruption to an important business service must be defined as an impact tolerance and metrics must be defined to monitor and measure the firm's ability to remain within the tolerance. Firms should articulate specific maximum levels of disruption, including time limits within which they will be able to resume the delivery of important business services following "severe but plausible" disruptions.

5 https://www.iaisweb.org/page/news/press-releases-prior-to-2014/file/87109/holistic-framework-for-systemic-risk

6 http://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/publication/2021/building-operational-resilience-impact-tolerances-for-important-business-services.pdf

7 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf

- **Mapping**: the resources that a firm deploys to deliver its most important services must be identified and documented across technology, data, people, facilities, suppliers and key dependent processes. Resiliency of the end-to-end supply chain of activities must be considered.
- **Testing**: firms should identify "severe but plausible" scenarios to test their ability to respond and recover within their impact tolerances.
- **Communication**: robust internal and external communication plans must be in place to manage the impact during any severe disruption, with an emphasis on ensuring the timeliness and accuracy of the information provided.
- **Recovery**: firms must demonstrate that they have taken decisive and effective actions to improve resilience and have embedded a recovery-centric mind-set within the organisation's culture.
- **Investing to build resilience**: firms should take ownership of their operational resilience and prioritise plans and investment choices based on their impacts on the public interest.

Operational resilience is again viewed as an outcome, and as a key factor in maintaining financial stability. It is also critical in supporting good customer outcomes and effectively managing conduct risk. The proposals aim to address risks to operational resilience, including those arising from the interconnectedness of the financial system and from the complex and dynamic environment in which firms operate. Final policy[8] was published in March 2021 and will come into force on 31 March 2022, with an implementation period of up to three years.

Work in progress — US and others

In November 2019, at the Bank Policy Institute Annual Meeting, John A. Beebe, Deputy Associate Director, LISCC, Federal Reserve Board of Governors noted[9] that the Federal Reserve Board (FRB) did not have an official definition or policy for operational resilience. However, he referred to the ability of banks to deliver critical operations through disruption and the familiar cyber resilience concepts of identifying, detecting and protecting against issues, then responding and recovering when an event occurs.

In the intervening period, things have moved on. The FRB now defines[10] operational resilience as: "*the ability to deliver operations, including critical operations and core business lines, through a disruption from any hazard. It is the outcome of effective operational risk management combined with sufficient financial and operational resources to prepare, adapt, withstand, and recover from disruptions.*"

In October 2020, the FRB, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency jointly issued a paper[11] entitled "Sound Practices to Strengthen Operational Resilience". This paper was aimed at US banks with more than USD 250 billion in total consolidated assets (or more than USD 100 billion in total assets and other risk characteristics) and covered a wide variety of topics such as governance and operational risk management, third party risks, IT resilience, cybersecurity, and scenario development. It did not revise existing or introduce new rules, but outlined practices drawn from existing regulations, guidance, statements and common industry standards to increase operational resilience. The paper notes that the practices "*are grounded in effective governance and risk management techniques, consider third-party risks, and include resilient information systems.*"

In December 2020, the European Central Bank (ECB) set out its expectations that major European banks would need to evolve in terms of overall operational resilience (not just cyber). The ECB intends to ensure that the requirements are coordinated with those of the UK and US regulators.

Operational resilience has been a proactive area of focus for the Australian prudential regulator (APRA) since the formation of its Operational Risk team in 1999. APRA defines[12] operational resilience "*as an entity's ability to withstand and recover from shocks*." It notes that a shock can be defined as an event that threatens the ability of an entity to provide business services or has disrupted the provision of business services. In extreme circumstances, this includes events which can compromise an entity's ongoing viability, such as the COVID-19 pandemic.

Since 1999, APRA has published prudential standards on Outsourcing, Business Continuity Management (BCM) and Risk Management, guidance on Pandemic Planning, Data Risk Management and Information Security (Cyber), and has issued an information paper on Cloud Computing. An Operational Resilience unit was established in 2020 and revisions and updates to the prudential standards and guidance on BCM, Outsourcing and Risk Management are expected in 2021. It is likely that these will be overlaid with further operational resilience requirements and/or guidance.

In June 2020, the Monetary Authority of Singapore issued[13] guidance and advisories to address operational, technology and cyber risks, but in the context of pandemic response rather than development of new requirements.

8 https://www.bankofengland.co.uk/prudential-regulation/publication/2018/building-the-uk-financial-sectors-operational-resilience-discussion-paper

9 https://bpi.com/wp-content/uploads/2020/01/112019-BPI-DEFINING-OPERATIONAL-RESILIENCE.pdf

10 https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm

11 https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1

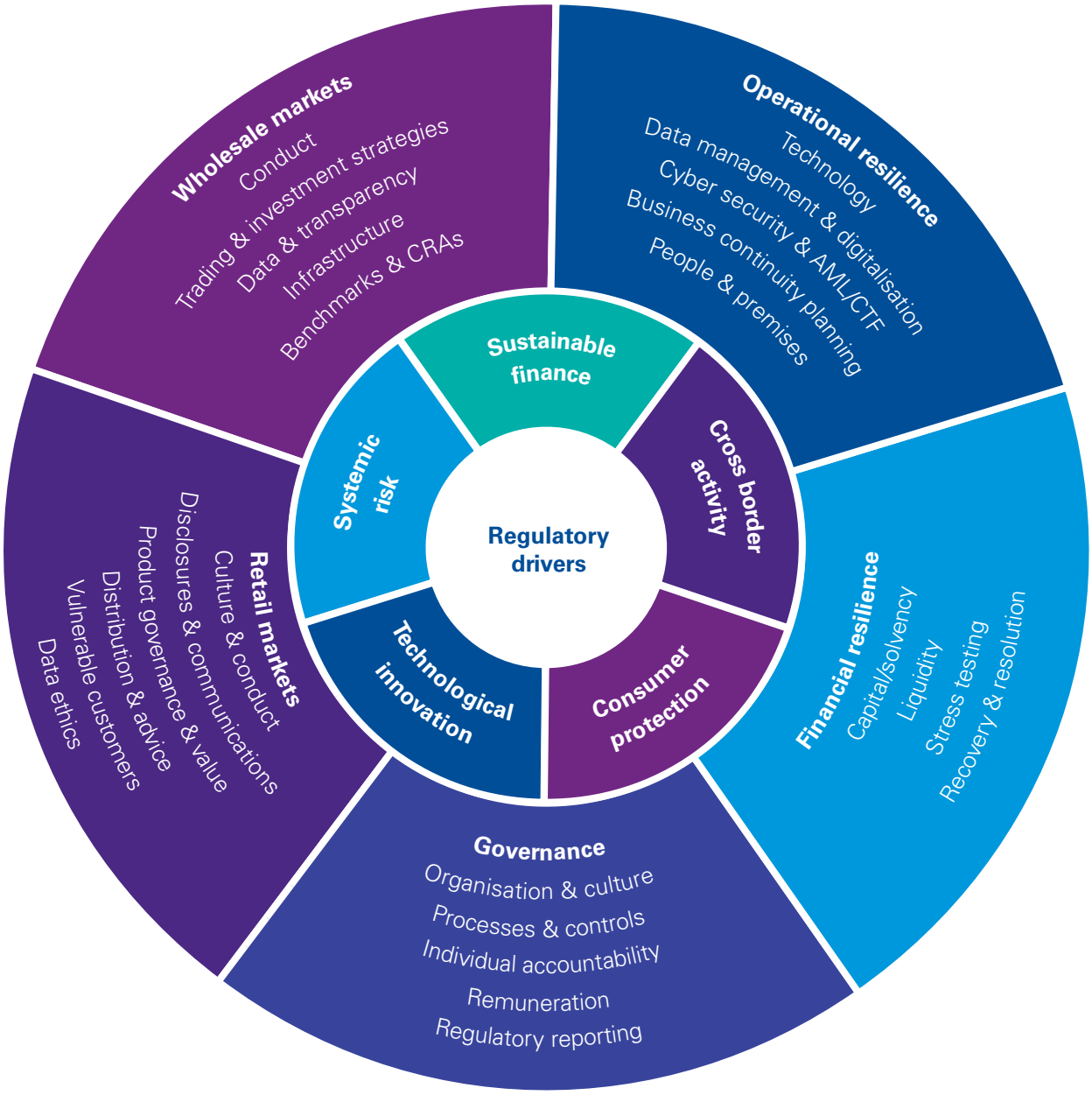
12 https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience

13 https://www.mas.gov.sg/regulation/covid-19/ensuring-safe-distancing-and-operational-resilience-of-the-financial-sector

In March 2021, this was expanded by a paper[14] on "Risk Management and Operational Resilience in a Remote Working Environment", which highlighted possible risks to financial institutions in the areas of operations, technology and information security, fraud and staff misconduct, and legal and regulatory risks.

And in the EU, which has long championed robust ICT security, digital operational resilience for all financial entities is now paramount (see Chapter 3).

Operational resilience in the new reality



Five key drivers are influencing priorities in regulatory agendas. Consumer protection and financial stability are the bulwarks of much financial services regulation, but the impacts of the pandemic and lock-down measures have brought additional topics to the fore. Volatility in capital markets has led to a renewed focus on systemic risk in relation to computer-led trading strategies and certain types of funds. Also, the pandemic has accelerated trends in the use of technology and demands for sustainable finance, and there are new challenges to doing business across borders. These three trends are now equally prominent drivers of regulatory priorities.

14 https://www.mas.gov.sg/-/media/MAS/News-and-Publications/Monographs-and-Information-Papers/Risk-Management-and-Operational-Resilience-in-a-Remote-Working-Environment.pdf

02. Focus on third-party risk

The FSB noted in November 2020 that financial institutions have relied on outsourcing and other third-party relationships for decades. However, it also pointed out that, in recent years, the extent and nature of interactions with "a broad and diverse ecosystem of third parties" have evolved, particularly in the area of technology. The financial sector's recent response to the impacts of the COVID-19 pandemic highlights the benefits as well as the challenges of managing the risks of financial institutions' interactions with third parties. The pandemic may also have accelerated the trend towards greater reliance on certain third-party technologies.

Financial services firms have turned towards outsourcing for the benefits that it offers in terms of costs, efficiency and expertise. Most financial firms are not infrastructure experts and, despite substantial programmes to streamline or re-organise their operations, they are, to a greater or lesser extent, encumbered by legacy systems. Equally, while transformation programmes are costly and complex for larger firms, smaller firms may simply not have the capability and resources internally to develop proprietary solutions.

Outsourcing may be an attractive option but third-party relationships present challenges. Regulators are concerned about:

- Concentration of providers
- Contractual terms, including exit terms and planning
- Data security
- Access rights and oversight, including governance, systems and controls
- Third parties' resilience, including BCP and disaster recovery
- Appropriate consideration of cultural alignment and embeddedness within the outsourcer
- Poor customer outcomes

Outsourcing principles for investment firms

In May 2020, IOSCO consulted[15] on new Principles on Outsourcing. These were based on existing 2005 and 2009 principles, expanded to include trading venues, market participants acting on a proprietary basis, credit rating agencies and FMIs. IOSCO notes that "*operational resilience refers to the ability of regulated entities, other firms such as service providers, and the financial market as a whole to prevent, respond to, recover, and learn from operational disruptions*".

The revised principles comprise a set of fundamental precepts and a set of seven principles. The fundamental precepts cover issues such as the definition of outsourcing, the assessment of materiality and criticality, their application to affiliates, the treatment of sub-contracting and outsourcing on a cross-border basis. The seven principles cover the following areas:

- Due diligence in the selection and monitoring of a service provider
- The contract with a service provider
- Information security, business resilience, continuity and disaster recovery
- Confidentiality issues
- Concentration of outsourcing arrangements
- Access to data, premises, personnel and associated rights of inspection
- Termination of outsourcing arrangements

IOSCO Principles on Outsourcing

Principle 1: A regulated entity should conduct suitable due diligence processes in selecting an appropriate service provider and in monitoring its ongoing performance.

Principle 2: A regulated entity should enter into a legally binding written contract with each service provider, the nature and detail of which should be appropriate to the materiality or criticality of the outsourced task to the business of the regulated entity.

Principle 3: A regulated entity should take appropriate steps to ensure both the regulated entity and any service provider establish procedures and controls to protect the regulated entity's proprietary and client-related information and software and to ensure a continuity of service to the regulated entity, including a plan for disaster recovery with periodic testing of backup facilities.

Principle 4: A regulated entity should take appropriate steps to ensure that service providers protect confidential information and data related to the regulated entity and its clients, from intentional or inadvertent unauthorised disclosure to third parties.

Principle 5: A regulated entity should be aware of the risks posed, and should manage them effectively, where it is dependent on a single service provider for material or critical outsourced tasks or where it is aware that one service provider provides material or critical outsourcing services to multiple regulated entities including itself.

Principle 6: A regulated entity should take appropriate steps to ensure that its regulator, its auditors, and itself are able to obtain promptly, upon request, information concerning outsourced tasks that is relevant to contractual compliance and/or regulatory oversight including, as necessary, access to the data, IT systems, premises and personnel of service providers relating to the outsourced tasks.

Principle 7: A regulated entity should include written provisions relating to the termination of outsourced tasks in its contract with service providers and ensure that it maintains appropriate exit strategies.

The systemic risk perspective

The FSB's discussion paper[16] on Regulatory and Supervisory Issues Relating to Outsourcing and Third-Party Relationships reflects many of the issues and challenges that firms face. It considers regulatory and supervisory issues relating to outsourcing and third-party relationships, with a particular focus on cloud and the concentration of cloud service providers.

There is concern about the possibility of systemic risk arising from concentration in the provision of some outsourced and third-party services to financial institutions. These risks will grow as the number of financial institutions receiving critical services from a given third party increases. Where there is no appropriate mitigant in place, a major disruption, outage or failure at one of these third parties could create a single point of failure with potential adverse consequences for financial stability and/or the safety and soundness of multiple financial institutions. Given the cross-border nature of this dependency, the FSB notes that supervisory authorities and third parties could particularly benefit from enhanced dialogue on the issue. The FSB has signalled that this paper will facilitate a discussion on current regulatory and supervisory approaches to the management of outsourcing and third-party risks.

15 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD654.pdf

16 https://www.fsb.org/2020/11/regulatory-and-supervisory-issues-relating-to-outsourcing-and-third-party-relationships-discussion-paper/

The FSB notes that contractual rights for financial institutions, their supervisors and the resolution authorities to access, audit and obtain information from third parties may be challenging to negotiate and exercise, particularly in a multi-jurisdictional context. The management of sub-contractors and supply chains was also highlighted in the context of financial institutions' response to the impacts of the COVID-19 pandemic. As part of its Fintech Action Plan, the European Commission intends to prescribe standard contractual clauses for outsourcing agreements.

The European approach takes shape

The European Supervisory Authorities (ESAs) have taken a largely coordinated approach to outsourcing guidance.

The European Banking Authority (EBA) published final guidelines on outsourcing arrangements[17] in February 2019, which incorporate earlier recommendations on cloud outsourcing. Importantly, outsourcing does not relieve the management body of its responsibility and it must retain the ability to make decisions related to outsourced business activities. Stricter requirements apply to outsourcing arrangements for critical or important functions. Firms must keep an updated register of all outsourcing arrangements, which if applicable must be at both a sub-consolidated and consolidated level, and these must be made available to national regulators as requested. Guidance on the outsourcing process is set out in detail, from pre-outsourcing analysis, through risk assessment and due diligence to the contractual phase, access, information and audit rights, termination rights, oversight of outsourced functions and exit strategies.

In February 2020, the European Insurance and Occupational Pensions Authority (EIOPA) issued final guidelines on outsourcing to cloud service providers[18] under the same 16 headings. These guidelines also require thorough risk assessment, due diligence and pre-outsourcing analysis. Where critical or important operational functions or activities are to be outsourced, this should be reflected in the insurer's risk profile in its own risk and solvency assessment (ORSA). Written notification, taking into account the principle of proportionality, should also be provided to the supervisory authorities.

A dedicated register of cloud outsourcing arrangements is required, including recently terminated arrangements, and contractual requirements should set out clearly the respective rights and obligations of the insurer and the cloud service provider. Contracts should include provisions for accessibility (including audit rights), availability of service, integrity, confidentiality, data privacy and safety and performance monitoring. In respect of audit rights, insurers may consider using third party certifications or internal audit reports made available by the cloud provider and/or pooled audits where the audit is performed jointly with other clients of the same service provider or where the audit is performed by a third-party appointed by them. Termination rights, oversight of outsourced functions and exit strategies are also covered.

17 https://eba.europa.eu/sites/default/documents/files/documents/10180/2551996/38c80601-f5d7-4855-8ba3-702423665479/EBA revised Guidelines on outsourcing arrangements.pdf
18 https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf

In June 2020, the European Securities and Markets Authority (ESMA) called for full audits of cloud providers and in December 2020 it published its final guidelines on outsourcing to cloud service providers[19], which will apply from July 2021. ESMA's nine guidelines are broadly aligned with the EBA and EIOPA and were also mindful of the European Commission's September 2020 proposal for a Digital Operational Resilience regulation (See Chapter 3). ESMA requires that firms put in place a specific strategy for any cloud outsourcing services, including appropriate governance arrangements and more stringent cyber security measures. Pre-outsourcing analysis and due diligence should be undertaken before appointing a provider and contracts must typically include specific terms relating to access and audit rights and subcontracting. Exit strategies (including planning and testing how a firm would migrate to another provider) should be considered before appointing a provider and an updated outsourcing register must be maintained and shared with regulators as requested.

Although the UK is no longer within the regulatory remit of the ESAs, the Prudential Regulation Authority (PRA) has included many of the provisions of the ESAs' guidelines in its proposals[20] and final policy[21] for outsourcing and third-party risk management. However, the PRA's requirements go broader and deeper than the ESAs, for example the ESAs focus primarily on outsourcing arrangements, while the PRA addresses all material third party arrangements. The PRA also requires firms to notify before a material outsourcing decision has been finalised and sets some further, more detailed, requirements on exit and contingency planning relating to stressed exit planning and scenarios testing of those exit plans. A follow-up consultation is planned, setting out detailed proposals for an online portal on which all firms would need to submit information on their outsourcing and third party arrangements.

Requirements around third party arrangements are becoming more onerous. The guidelines and regulations around governance, oversight and documentation may be challenging for smaller firms. The need to deliver specific outsourcing or cloud strategies may be outside the capability of some firms, which will need to seek external guidance.

Key considerations for firms:

- Governance and record keeping
- Assessing materiality and inherent risks
- Pre-contract due diligence
- Risk based contractual clauses
- Security and data controls
- Ongoing risk assessments
- Access and audit rights
- Managing sub-contractor risks
- Exit planning and contingency
- Linkages to operational resilience programme

19 https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf
20 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/cp3019.pdf
21 https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2021/march/ps721.pdf

03. Towards digital resilience - the next level

Cyber resilience has long been the backbone of resilience programmes and continues to be of critical importance. However, in the new reality, the focus is expanding to the broader ICT risk environment, and the EU has introduced a technology-driven definition of "digital operational resilience".

Cyber and ICT resilience - the building blocks

There has long been a strong focus on cyber resilience and ICT risk, as the foundations for ensuring business continuity in the financial sector. In the four years before the pandemic, many frameworks and guidelines were issued, which are now being updated and expanded.

Much cyber regulation is industry agnostic, for example the EU's 2016 Networks and Information Security (NIS) Directive, the global NIST (National Institute of Standards and Technology) Cybersecurity Framework and the European Commission's 2020 EU Cybersecurity Strategy. However, more targeted provisions for financial services have also developed. NIS is due to be extended to cover additional sectors and place stricter requirements on "essential entities," including financial services and cloud and data service providers, and there are specific requirements for EU banks as part of the ICT Supervisory Review and Evaluation Process.

In 2016, the Committee on Payments and Market Infrastructures (CPMI) and the Board of IOSCO jointly issued[22] guidance on cyber resilience for financial market infrastructures. This set out internationally agreed guidance on topics such as:

- The importance of board and senior management attention in sound cyber governance
- The ability to resume operations quickly and safely after a successful cyber-attack
- The need to make use of good-quality threat intelligence and rigorous testing
- Instilling a culture of cyber risk awareness and demonstrating ongoing re-evaluation and improvement of their cyber resilience at every level within the organisation
- Cyber resilience as a collective endeavour of the whole ecosystem

In 2017, the FSB published[23] a Summary Report on Financial Sector Cybersecurity Regulations, Guidance and Supervisory Practices, to promote cross-border cooperation. This was followed by a Cyber Lexicon[24] in 2018, which included a set of approximately fifty core terms relating to cyber security and cyber resilience in the financial sector.

The FSB's October 2020 toolkit[25] for financial institutions includes 49 practices for effective cyber incident response and recovery across seven components: governance, planning and preparation, analysis, mitigation, restoration and recovery, coordination and communication, and improvement. As part of its 2021 workplan, the FSB will also explore the scope for convergence in the regulatory reporting of cyber incidents and the need for revisions to the FSB Cyber Lexicon.

22 https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

23 https://www.fsb.org/2017/10/summary-report-on-financial-sector-cybersecurity-regulations-guidance-and-supervisory-practices/

24 https://www.fsb.org/2018/11/cyber-lexicon/

25 https://www.fsb.org/2020/10/fsb-encourages-use-of-cyber-incident-response-and-recovery-toolkit/

The EU introduced its TIBER-EU Framework in May 2018 (Threat Intelligence-based Ethical Red Teaming), developed jointly by the ECB and EU national banks, and applicable to (supra)national authorities and entities that form the core financial infrastructure. In the UK, larger regulated firms are subject to CBEST penetration testing, created by the Bank of England and supported by the Council for Registered Ethical Security Testers (CREST).

At the end of 2018, the ECB published[26] its cyber resilience oversight expectations for financial market infrastructures, and the US Securities and Exchange Commission published[27] Cyber Security and Resiliency Observations in January 2020.

The EU also has established sources of guidance on ICT risk. In May 2017, the EBA issued[28] Final Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process. These were followed[29] by Final Guidelines on ICT and security risk management in November 2019. For insurers, EIOPA's consultation[30] on ICT security and governance closed in March 2020. At the national level, requirements such as the German regulator's "BAIT[31]" and the Dutch Central Bank's IT principles formalised local supervisory expectations and provided a framework for firms to implement minimum requirements for IT risk management.

A broader view – the road to DORA

The European Commission has published[32] a wide-ranging draft regulation on digital operational resilience for the financial sector (DORA). This builds on existing regulatory expectations around operational resilience but focuses on the ability of firms to build, assure and review their operational integrity from a technological perspective. DORA will establish a comprehensive EU framework with rules for all regulated financial institutions. It will:

— Streamline and upgrade existing financial legislation and introduce new requirements where gaps exist, for example by:

- Better aligning firms' business strategies and the conduct of ICT risk management, thereby improving overall management of ICT risks and ensuring firms can assess the effectiveness of their preventive and resilience measures and identify ICT vulnerabilities
- Applying testing requirements proportionately, depending on a firm's size, business and risk profile
- Strengthening firms' oversight and ensuring sound monitoring of third-party ICT
- Raising awareness of ICT risk and minimising its spread through information-sharing, including allowing firms to exchange cyber threat information and intelligence

— Create more coherent and consistent incident reporting mechanisms, to reduce administrative burdens for firms and strengthen supervisory efficiency by:

- Harmonising and streamlining the reporting of ICT-related incidents
- Increasing supervisors' knowledge of threats and incidents by enabling them to access relevant information

There may be trouble ahead…

It is difficult to disagree with any of the stated aims of DORA. However, agreement of the proposals is far from a done deal and implementation across the EU may be challenging. Already, several potential issues are emerging, not least the need for DORA to interact or co-exist with other guidelines and legislation. DORA will require amendments to a wide range of existing financial services legislation, including MiFID II, Solvency II, UCITS and AIFMD. It is not yet clear how these interactions and amendments will be implemented, particularly where existing guidelines have been agreed but are not yet fully in force.

> "Digital operational resilience means the ability of a financial entity to build, assure and review its operational integrity from a technological perspective by ensuring, either directly or indirectly, through the use of services of ICT third-party providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity makes use of, and which support the continued provision of financial services and their quality."

In addition, the scope is vast. Over 30 types of financial entity are covered with only minor concessions to proportionality. Proposals for ICT risk management, including the management of third-party risk, will be complex to implement. The reporting of major incidents and enforcement processes require further clarification. Detailed rules and guidance to be issued by the ESAs may provide some clarity but are unlikely to mitigate all the challenges.

26 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

27 https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

28 https://eba.europa.eu/sites/default/documents/files/documents/10180/1841624/ef88884a-2f04-48a1-8208-3b8c85b2f69a/Final Guidelines on ICT Risk Assessment under SREP (EBA-GL-2017-05).pdf

29 https://eba.europa.eu/sites/default/documents/files/documents/10180/2522896/32a28233-12f5-49c8-9bb5-f8744ccb4e92/Final Guidelines on ICT and security risk management.pdf

30 https://www.eiopa.europa.eu/content/consultation-proposal-guidelines-information-and-communication-technology-ict-security-and_en

31 Bankaufsichtlichen Anforderungen and die IT

32 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0595&from=EN

A joint letter[33] from the chairs of the ESAs in February 2021 agreed with the main principles of DORA and the need to establish a comprehensive EU framework. It also supported the call for enhanced collaboration and co-operation among authorities within the EU and internationally. However, the ESAs raised concerns around their proposed roles in overseeing Critical Third Party Providers (CTTPs), in particular the challenges of overseeing cross-sectoral CTTPs within the ESAs' individual sector-specific remits.

They also flagged the mismatch of powers given to them - once an ESA has issued a recommendation, the relevant competent authority will be responsible for follow-up and taking any enforcement action. Such action could include requiring supervised financial entities temporarily to suspend CTPP services or terminate contracts with a CTPP. Finally, they noted the need for adequate resources to undertake their new responsibilities and the need for further proportionality in implementation.

DORA is likely to evolve as it goes through the EU's legislative procedure. The final version can be expected in the next 18 to 24 months. In the meantime, financial entities and ICT service providers should be mindful of the significant changes in regulatory requirements around operational resilience that are likely to be introduced and should begin assessing how these will impact their ICT risk management frameworks.

Key challenges of DORA

Scope – wide range of entities, one-size-fits-all approach, limited proportionality

Implementation – interaction with existing guidelines and legislation unclear; will applydirectly to vendors

ICT risk management – detailed requirements may limit flexibility and agility; could drive fragmentation in technology estate

Third party ICT risk – perscriptive requirements will be challenging for smaller firms and legacy systemd; definitions of critical providers unclear

Triage & major incident reporting – need for clarity and consistency around reporting requirements; location-specific requirements may hinder incident management; triage burden on national regulators

Enforcement – wide enforcement powers may lead to compensation issues and disruption; open to national interpretation and application

33 https://www.esma.europa.eu/sites/default/files/library/esa_2021_07_letter_dora_oversight.pdf

04. Variations on a theme

Recent regulatory announcements on operational resilience have been high profile and much has been made of the differences in terminology and possible political agendas, which might underpin observed nuances in regulatory statements.

It is certainly true that a single view of the world could enable simpler decision-making and planning for firms, particularly global firms subject to multiple regimes, but it is to be expected that there will be differences in approach and taxonomy from one regulator to another and from one geography or jurisdiction to another.

Linguistic differences

There are differences in the language used in different publications. BCBS refers to **"critical operations"** versus the UK definition of **"important business services"**. "Critical operations" is based on the Joint Forum's 2006 high-level principles for business continuity and borrows from the terminology used in recovery and resolution. It encompasses **"critical functions"** as defined by the FSB, expanded to include "*activities, processes, services and their relevant supporting assets the disruption of which would be material to the continued operation of a bank or its role in the financial system*".

In the UK, a **"business service"** is a service that a firm provides to an external end user or participant. Business services qualify as **"important"** when their failure could cause an intolerable level of harm to consumers or market participants, harm to market integrity, or threaten policyholder protection, the safety and soundness of individual firms, or financial stability.

In the US, the FRB defines **"critical operations"** and **"core business lines"**, the first referring to operations whose failure or disruption could pose a threat to the financial stability of the US and the second where failure would result in a material loss of revenue, profit or franchise value for the firm.

There is no concept of **impact tolerances** in the US or EU proposals, whereas this is a cornerstone of the UK approach. The UK proposals define impact tolerances as "*tolerance for disruption, under the assumption that disruption to a particular business service will occur*". The UK regulators stress that impact tolerances are not the same as risk appetite metrics.

But, most importantly, the definitions of operational resilience are almost identical – BCBS highlights the "ability to recover from disruptive events" and the UK regulators require firms to "respond and adapt to, as well as recover and learn from, disruptive events".

Common goals, different perspectives

Regulatory requirements for outsourcing and third-party risk are well-aligned across sectors and geographies as discussed in Chapter 2. On broader operational resilience issues, regulators and industry bodies are focused on common goals, such as:

- Greater accountability and ownership, with engagement from the top down
- Clear definition of a firm's key business activities
- Understanding the key dependencies required to deliver those activities
- Testing resilience under stress scenarios
- Defining meaningful metrics to quantify resilience and assess tolerances for disruption
- Ensuring timely and appropriate communications for customers, policyholders or investors

BCBS, representing 28 jurisdictions and 45 institutions, has set out high level principles ranging from governance to business continuity and incident management. It has explicitly stated that operational resilience will require management and reduction of risks to ensure continuity of critical operations. However, it will fall to national authorities to decide whether to take a more prescriptive approach.

The UK has opted to set out a detailed framework for operational resilience with more specific requirements for firms and clear expectations for forward monitoring by supervisors. This can be viewed against a background of highly publicised resilience failures since the 2008 crisis and escalating threats from a variety of sources. The UK regulators also place significant emphasis on consumer harm and the potential for operational resilience failures to create conduct issues, perhaps reflecting the dual-regulatory approach in the UK. Delivery against the UK proposals would also deliver against the BCBS principles for banks.

In the EU and the US, conversations around operational resilience often take place within the Risk function. In certain cases, it is mandated that specific responsibilities, for example under the EBA ICT guidelines, sit within Risk. However, in assigning accountability for operational resilience to the Chief Operations rather than the Chief Risk function, the UK approach is agnostic to which line of defence bears responsibility. Instead, in an increasingly digital world, the intention is to empower technology roles and encourage a less siloed view, enabling firms to take a true service-based view of their most important activities. This extends to third-party risk management which has traditionally been viewed as a procurement activity but is now fundamental to the continuing operations of many financial services firms.

Cutting through the noise

Firms must be mindful of differences in definitions as they develop their approaches to operational resilience. However, rather than demonstrating divergence in intent, such differences more likely reflect differences in how jurisdictions have chosen to codify and/or how the regulation has evolved. Excessive focus on the variations in language and format might suggest that firms are taking an overly compliance-based approach.

To focus on whether one position is clearer or better than another is to miss the point somewhat. What all the regulators are targeting, regardless of their specific supervisory requirements or definitions, is **a financial services sector that is more resilient to operational disruption, hence reducing the potential for wider contagion, financial instability and harm to end-customers.**

05. Looking ahead and lessons learned

COVID-19 has not changed the direction of travel from a regulatory perspective. If anything, it has accelerated the regulatory drive to push ahead, as evidenced by publication of the EU's DORA and other guidance. According to the European Commission, at the beginning of the COVID-19 pandemic, the use of financial applications in Europe increased[34] by 72% in a week, and during the pandemic cyberattacks on financial institutions rose by 38%. These figures point to a clear and continuing need for robust operational resilience.

The BCBS principles and DORA incorporate learning from COVID-19, whereas the UK consultations were published pre-pandemic. However, none of the UK concepts were diluted in the final policy statements, and regulators around the world continue to reinforce the importance of operational resilience.

Firms are grappling with a common set of implementation challenges, including how best to:

- Achieve not just short-term regulatory compliance, but also strategic resilience, by creating a scalable and sustainable operating model for the longer term, developing true accountability and embedding a resilience culture
- Balance global consistency versus local finish - where aspects of operational resilience do not apply equally to all regulated entities in a group, how should this be managed?
- Achieve an appropriate balance of narrow and broad service definition, completeness and granularity
- Calibrate intolerable harm and impact tolerances – these are new concepts and will take some time to land
- Look to the future and harness the potential of digital resilience

Regulators are cognisant of the dangers of regulatory fragmentation and are co-operating where possible. The Bank of England is leading on the FSB's work on outsourcing arrangements and was involved in development of the BCBS principles. The ECB and PRA have also committed to working together with each other and the FRB to ensure the implementation of well-coordinated supervisory approaches. Regulators face challenges too, not least ensuring that they have the expertise to supervise effectively, given the likely requirements for new skillsets.

Significant questions remain, for example:

- What does good look like when not all firms have the same structure?
- What will regulators do with the data they gather?
- Will there ultimately be capital charges and mandated resilience stress tests?
- Could such tests lead to sanctions for poor performers and what would the potential reputational implications be?
- How far could or should the regulatory perimeter be extended to bring other entities within the scope of requirements?

A few years ago, all the conversations were about cyber resilience. Now firms are discussing not only cyber, but disruptors such as pandemics and climate events in the context of resilience. There is more work to do to ensure system-wide resilience to all the potential hazards that could pose risks to the financial system. Through continued co-operation, regulators may be better able to identify areas where global standards and convergence can be explored.

Regulatory requirements will likely be demanding and wide-reaching, but fundamentally, the underlying messages are the same – **operational resilience is critical to an organisation's success and sustainability and regulators view it as a boardroom agenda. Firms must act now to future-proof their businesses.**

Look out for the final paper in this thought leadership series that will consider other 'new reality' issues.

34 https://ec.europa.eu/info/publications/200924-digital-finance-proposals_en

Contact us

Francisco Uria Fernandez
EMA Head of FS and Banking & Capital Markets
T: +34 9145 13067
E: furia@kpmg.es

Karim Haji
UK Head of Financial Services
T: +44 20 7311 1718
E: karim.haji@kpmg.co.uk

Michelle Adcock
EMA FS Regulatory Insight Centre
T: +44 20 3306 4621
E: michelle.adcock@kpmg.co.uk

Philip Deeks
EMA FS Regulatory Insight Centre
T: +44 20 7694 8545
E: philip.deeks@kpmg.co.uk

Andrew Husband
Partner, Powered Resilience Leader
KPMG in the UK
T: +44 20 7694 1040
E: andrew.husband@kpmg.co.uk

James Lewis
Co-Head of EMA FS Regulatory Insight Centre
T: +44 20 7311 4028
E: james.lewis@kpmg.co.uk

Kate Dawson
EMA FS Regulatory Insight Centre
T: +44 20 7311 8596
E: kate.dawson@kpmg.co.uk

Julie Patterson
EMA FS Regulatory Insight Centre
T: +44 20 7311 2201
E: julie.patterson@kpmg.co.uk

home.kpmg/regulatorychallenges

CREATE | CRT134865 | March 2021