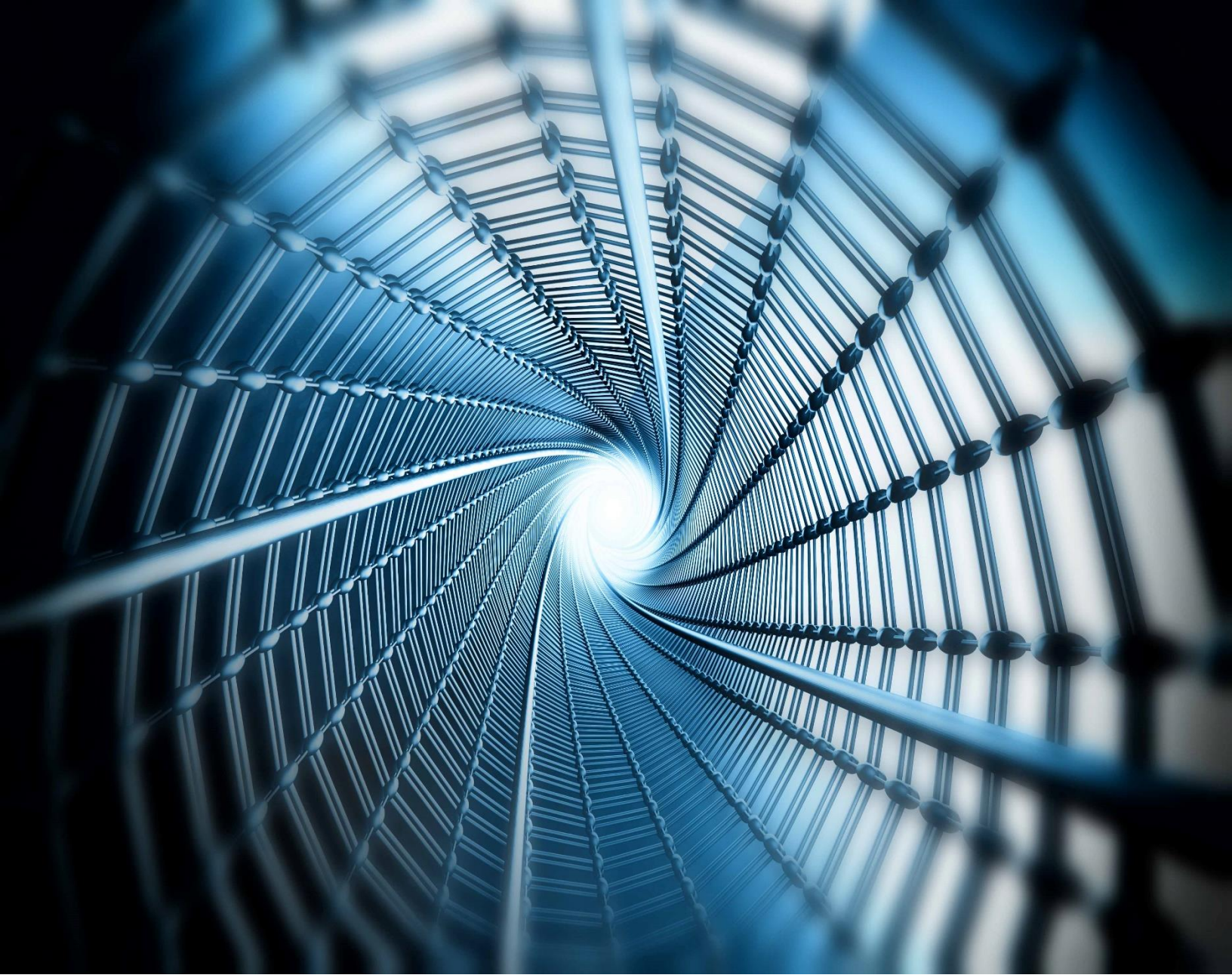

Operational Resilience – Global Regulatory Developments and J.P. Morgan Industry Engagement

July 2022

J.P.Morgan

Operational Resilience – Global Regulatory Developments and J.P. Morgan Industry Engagement

Evolution of Global Operational Resilience Regulatory Landscape

Operational resilience has been a focus area for regulators globally over the past several years, with high-profile cybersecurity incidents, IT systems outages, natural disasters, geopolitical events and a global COVID-19 pandemic highlighting the importance of being able to continue and quickly restore business services. This focus has been amplified by the global, interconnected nature of financial services.

While regulators may be using slightly different terminologies to define operational resilience, they have one common expectation towards the financial services sector: improved ability to withstand shocks in order to deliver critical services[1] through sudden disruptions. As operational risk is inherent to the financial services' business activities, a robust operational resilience framework is meant to enable financial firms (firms) to recover their critical services in the event of a business interruption. There is also acknowledgement by regulators that effective management of operational risk (across the individual risk management disciplines including cyber, technology, data, third-party outsourcing and business resiliency) leads to operationally resilient outcomes.

In the past, firms were by and large reliant on business continuity plans (BCP) and disaster recovery (DR) to deal with disruptions, and these were typically designed and performed on critical functions and systems within each organizational silo. Operational resilience regulations are changing this by requiring firms to approach business continuity of critical services on a holistic basis spanning across all supporting functions and assets (i.e. people, processes, technology, facilities and information). Operational disruptions and the unavailability of critical services have the potential to cause wide-reaching harm to consumers and/or risk to market integrity, threaten the viability of firms and cause instability in the financial system. Through implementation of robust operational resilience policies, regulators aim to minimize impact on market integrity, financial stability and consumers.

In a clear signal of growing importance of operational resilience, at the end of 2020 the European Central Bank (ECB), the US Federal Reserve Bank and the U.K. Prudential Regulation Authority (PRA) committed[2] to working together to ensure the implementation of well-coordinated supervisory approaches on operational resilience. While the world's leading prudential regulators acknowledged that the financial sector had made progress in enhancing operational resilience over recent years, they highlighted that more remained to be done to ensure that firms are resilient to potential operational disruptions from all hazards which could pose risks to the wider financial system.

There has been evidence of concerted efforts to encourage international alignment and coordination of operational resilience policies and best practices, in order to reduce likelihood of conflicting requirements for firms operating in multiple jurisdictions. Leveraging lessons learned from the COVID -19 pandemic, in March 2021 the Basel Committee on Banking Supervision (BCBS) published its Principles for Operational Resilience (POR)[3] which build on the BCBS principles for the sound management of operational risk, originally promulgated in 2003 and most recently updated last year. POR serve as the foundation and guide for regulators as they develop their own operational resilience approaches and various jurisdictions have been aligning their national policies to the BCBS standard. The Financial Stability Board (FSB) has also been driving greater convergence in practices related to cyber incident reporting and outsourcing/third-party risk management[4][5]. Earlier

[1] Also known as: important business services (UK), critical operations (US), critical or important functions (EU)

[2] https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2020/ssm.2020_Statement_regarding_supervisory_cooperation_on_operational_resilience.en.pdf?85a35cc5de0ec2aae77f0f562a70f582

[3] https://www.bis.org/bcbs/publ/d516.htm

[4] https://www.fsb.org/2021/10/cyber-incident-reporting-existing-approaches-and-next-steps-for-broader-convergence/

[5] https://www.fsb.org/2021/06/outsourcing-and-third-party-risk-overview-of-responses-to-the-public-consultation/

this year, the European Systemic Cyber Group (ESCG) issued a recommendation to establish a pan-European systemic cyber incident coordination framework[6]. In the meantime, members of the G7 Cyber Expert Group are focusing on working together on addressing the escalating shared threat from criminal ransomware networks[7].

Over the last two years, promulgation of operational resilience policy has gained substantial traction globally. New standards and consultations are continually being proposed across multiple jurisdictions, with impacts on a variety of firms including banks, assets managers, institutional investors, financial market infrastructures (FMIs) and third-party vendors. Despite targeted efforts by the governments and regulators to facilitate international policy alignment, there are differences on a regional and national level in terms of how regulators approach operational resilience, and this inevitably poses challenges for firms with global operating models.

In this briefing, we discuss several key policy developments of relevance to J.P. Morgan and our clients as well as provide an update on how J.P. Morgan is engaging with the regulators and the industry on this important topic.

United Kingdom

Globally, the UK positioned itself as a pioneer as it considers operational resilience holistically (bringing together all disciplines and all threats) and other jurisdictions have been paying close attention to this approach. 2022 has been a pivotal year for the UK's financial sector as after years of policy development and planning, firms now need to put into practice their work on operational resilience frameworks. In line with the **Financial Conduct Authority (FCA)/Bank of England (BOE)/PRA rules on operational resilience**[8], by March 31st of this year, firms must have identified their critical services, set impact tolerances for the maximum tolerable disruption and carried out mapping and testing to a level of sophistication necessary to do so. In addition, firms must have identified any vulnerabilities in their operational resilience. As soon as possible after 31st of March 2022, and by no later than 31st of March 2025, firms must perform mapping and testing so that they are able to remain within impact tolerances for each critical service. Firms must also make the necessary investments to enable them to operate consistently within their impact tolerance.

Operational resilience of the FMIs is another growing area of focus for the UK regulators. Given key dependency by financial firms on the FMIs (central clearing counterparties (CCPs), central securities depositories (CSDs), recognized payment system operators (RPSOs) and specified service providers (SSPs)), the Bank of England has recently published plans to bolster rules around **outsourcing and third-party risk management in FMIs**[9].

As the UK's financial services sector has been becoming increasingly reliant on cloud and other-third party providers (outside of the financial sector), the UK Government is considering legislation to support resilient outsourcing to technology providers. In June 2022, Her Majesty's Treasury (HMT) published a policy statement[10] announcing the intention to legislate a new **critical third-party regime** and indicating a forthcoming discussion paper from the UK regulators.

These initiatives undertaken by the UK authorities signal a shift in regulators' expectations over operational resilience in financial services and their desire for continuity of critical services across the sector – regardless of the way they are delivered.

---

[6] https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html
[7] https://www.gov.uk/government/publications/g7-interior-and-security-senior-officials-meeting-on-ransomware
[8] https://www.fca.org.uk/publications/policy-statements/ps21-3-building-operational-resilience
[9] https://www.bankofengland.co.uk/paper/2022/boe-consultation-papers-fmi-outsourcing-and-third-party-risk-management
[10] https://www.gov.uk/government/publications/critical-third-parties-to-the-finance-sector-policy-statement/critical-third-parties-to-the-finance-sector-policy-statement

European Union

The EU policymakers have been cooperating with their counterparts globally and developing their own approach to operational resilience. In May of this year, the EU policymakers reached a political agreement on the Digital Operational Resilience Act (DORA) which has been going through the legislative process since it was originally proposed in 2020. DORA will codify into law requirements around Information and Communications Technology (ICT) security risk management and the management of third-party ICT providers that are, to some extent, already contained in a suite of guidelines produced by the EU's supervisory authorities (ESAs). With the core aim of reducing ICT risk, the significance of DORA is that it harmonizes obligations for the financial institutions (almost all areas of financial services will be in scope) in areas mentioned above as well as the reporting of major ICT-related incidents and conducting threat-led penetration testing. Additionally, for the first time, there will be a direct oversight regime for the major technology providers to financial entities.

Similar to the UK and other jurisdictions, in the EU financial services sector there has been increasing use of cloud services over the recent years. In recognition of this, by the end of 2022 the EU-based firms are expected to adhere to **ESMA's guidelines on outsourcing to cloud service providers**[11] and ensure they meet the requirements related to: contractual terms with outsourced providers; information security; access and audit rights; sub-outsourcing; and supervision of cloud outsourcing agreements. Additionally, through its **2019 Guidelines on outsourcing arrangements**[12], **the European Banking Authority (EBA)** enhanced its expectations for in scope firms in the context of cloud services and ICT risk. The **European Insurance and Occupational Pensions Authority (EIOPA)** also published is own guidelines on outsourcing to cloud providers in 2020[13]. It remains to be seen how these existing regulations will interact with DORA in the context of practical implications for the firms as they operationalize regulatory requirements and take steps to ensure ongoing compliance.

In another key development, Ireland has become the first EU member state to set out a holistic policy on operational resilience similar to the one pioneered by the UK. By the end of 2023, the Irish financial sector is expected to comply with the **Central Bank of Ireland's Cross Industry Guidance on Operational Resilience CP140**[14] published at the end of 2021. The guidance sets out how Irish-based firms should prepare for; respond to; and recover and learn from an operational disruption that affects the delivery of critical or important business services.

Asia Pacific

While in the jurisdictions such as the UK regulators have been prioritizing operational resilience policies focused on critical services, in the Asia Pacific region strengthening of the ICT and technology risk management regulatory frameworks has been a key priority of the policymakers.

In Singapore, signaling importance of the technology risk management (TRM), in 2021 the Monetary Authority of Singapore (MAS) published revised TRM guidelines[15] which set out technology risk management principles and best practices for the financial sector, to guide firms when it comes to establishing sound and robust technology risk governance/oversight and maintaining cyber resilience. Building on this, in April 2022 the Parliament of Singapore passed new laws[16] which provided MAS with new powers to enforce technology risk management requirements for financial institutions. Most recently, in June 2022 MAS published revised Guidelines on Business Continuity Management (BCM)[17] for firms in order to help them

[11] https://www.esma.europa.eu/press-news/esma-news/esma-publishes-cloud-outsourcing-guidelines
[12] https://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-outsourcing-arrangements
[13] https://www.eiopa.europa.eu/document-library/guidelines/guidelines-outsourcing-cloud-service-providers_en
[14] https://www.centralbank.ie/docs/default-source/publications/consultation-papers/cp140/cross-industry-guidance-on-operational-resilience.pdf
[15] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulatory-and-Supervisory-Framework/Risk-Management/TRM-Guidelines-18-January-2021.pdf
[16] https://www.mas.gov.sg/news/speeches/2022/explanatory-brief-for-financial-services-and-markets-bill-2022
[17] https://www.mas.gov.sg/regulation/guidelines/guidelines-on-business-continuity-management

strengthen their resilience against service disruptions arising from IT outages, pandemic outbreaks, cyber-attacks and physical threats. The revised framework takes into account learnings from the handling of the COVID-19 pandemic and increased digitalization in the financial sector.

In addition to the focus on the ICT and TRM regulatory priorities, regulators in the Asia Pacific region have also been taking steps to align to the latest international operational resilience rules and best practices. Following a public consultation, in May 2022 the Hong Kong Monetary Authority (HKMA) published two sets of rules[18] - new guidelines on operational resilience and revised guidelines on business continuity planning - which essentially transpose BCBS's POR issued in March 2021. Prior to this, in 2021 the Securities and Futures Commission (SFC) also published a circular and a report on operational resilience and remote working[19], with standards and guidelines for implementation of an effective operational resilience framework.

In Australia, the Australian Prudential Regulation Authority (APRA) has continued to uplift its standards for the financial services sector by: implementing enhanced information security framework CPS 234 in 2019; establishing an Operational Resilience Unit in 2020; ensuring operational resilience forms part of its 2021-2022 policy priorities with a consultation on operational risk management envisaged for 2022[20]. A software upgrade leading to a day-long outage of the Australian Securities Exchange (ASX) in 2020 also prompted the Australian Securities and Investments Commission (ASIC) to review and eventually upgrade standards on technological and operational resilience. Subsequently, in March 2022, ASIC published a set of rules[21] (commencing from March 2023) introducing additional obligations on market participants and operators in relation to technological and operational resilience; reinforcing the broader regulatory focus on deterring inadequate systems and operational governance and controls; seeking to create greater alignment with international standards and other domestic standards.

United States

In the US, regulators are taking steps to modernize their guidance on operational resilience, with US federal regulators publishing a joint paper outlining sound practices to strengthen operational resilience, and the Securities and Exchange Commission (SEC) publishing proposed cybersecurity risk management regulation and increasing focus on operational resilience through examination.

On October 30, 2020, **the US federal banking regulators[22] issued guidance[23] (the Guidance) on sound practices for the largest US banking organizations to strengthen their operational resilience**, including with respect to cyber risk management. The Guidance describes seven categories of sound practices that US banking organizations may use to strengthen and maintain their operational resilience: governance, operational risk management, business continuity management, third-party risk management, scenario analysis, secure information system management, and surveillance and reporting. The Guidance was drawn from existing regulation, guidance, statements and is largely consistent with the BCBS final Principles for Operational Resilience[24].

[18] https://www.hkma.gov.hk/media/eng/doc/key-information/guidelines-and-circular/2022/20220531e1.pdf
[19] https://apps.sfc.hk/edistributionWeb/gateway/EN/circular/intermediaries/supervision/doc?refNo=21EC41
[20] https://www.apra.gov.au/covid-19-a-real-world-test-of-operational-resilience
[21] https://asic.gov.au/about-asic/news-centre/find-a-media-release/2022-releases/22-045mr-asic-amends-market-integrity-rules-and-other-asic-made-rule-books/
[22] The US banking regulators are the Board of Governors of the Federal Reserve System ("Federal Reserve"), Office of the Comptroller of the Currency ("OCC"), and Federal Deposit Insurance Corporation ("FDIC")
[23] https://www.federalreserve.gov/newsevents/pressreleases/bcreg20201030a.htm
[24] https://www.bis.org/press/p200806.htm

Operational Resilience – Global Regulatory Developments and J.P. Morgan Industry Engagement

More recently, the SEC promulgated **proposed new cybersecurity risk management regulations** for:

- Public companies[25] - the proposed rules would require each public company to report material cybersecurity incidents within four business days after determining that it has experienced such incidents, provide periodic updates of previously reported cybersecurity incidents, describe its cybersecurity risk management policies and procedures, disclose its cybersecurity governance practices and disclose cybersecurity expertise on the board of directors;
- Registered advisers and funds[26] - the proposed rules would require advisers and registered funds to complete written cybersecurity risk assessments, develop certain cybersecurity policies and procedures, and implement cybersecurity incident reporting and cyber incident record-keeping.

[25] *https://www.sec.gov/rules/proposed/2022/33-11038.pdf*
[26] *https://www.sec.gov/rules/proposed/2022/33-11028.pdf*

J.P. Morgan Industry Engagement and Regulatory Advocacy

J.P. Morgan is committed to providing high quality and operationally resilient services to best serve our customers, clients and communities. As the operational resilience regulatory landscape continues to evolve, we recognize that not only do we need to meet our own obligations, but in some instances, we have a role to play in supporting our clients in helping them meet their regulatory requirements.

Given the interconnectedness of the financial services sector, international coordination and engagement among multiple stakeholders including governments, regulators, banks, investment managers, institutional investors, FMIs, and shared utilities is critical to supporting consistent implementation of operational resilience policies and frameworks. To this point, fragmented regulatory regimes and approaches pose a fundamental challenge for the efficient management and mitigation of risks across operational resilience.

In light of the continued regulatory and industry focus on operational resilience, and the need for international coordination and engagement across the entire sector, J.P. Morgan has been engaging globally with the industry and policymakers on relevant legislative and regulatory developments.

For example, J.P. Morgan has been actively working with the industry associations globally, including the Institute of International Finance (IIF), Global Financial Markets Association (GFMA), Securities Industry and Financial Markets Association (SIFMA), Association for Financial Markets in Europe (AFME), Asia Securities Industry & Financial Markets Association (ASIFMA) and Association of Global Custodians (AGC) across a number of regulatory consultations and proposed policies discussed earlier in this briefing.

J.P. Morgan's engagement in industry and regulatory discussions in the UK is an example of our focus on this topic. Following the publication of the Operation Resilience discussion paper by the UK authorities (BoE/PRA/FCA) in 2018, J.P. Morgan worked with industry peers and the UK authorities to help shape an effective and comprehensive implementation of the policy objectives within that discussion paper. J.P. Morgan's initial response to the discussion paper was to conduct pilots across a number of business areas at J.P. Morgan in order to provide practical experience of implementing the new concepts in the discussion paper, such as important business services and impact tolerance. J.P. Morgan provided feedback both directly to the UK authorities and indirectly via the trade association, UK Finance, on the 2018 discussion paper and consultation papers that followed in 2019.

Following the initial pilots and acknowledging the benefits of the UK's authorities' holistic approach to operational resilience, in 2020 J.P. Morgan expanded its implementation of the BOE/PRA/FCA operational resilience standards to a firm-wide initiative. That resulted in J.P. Morgan being well positioned to accommodate the final BOE/PRA/FCA operational resilience policy published in March 2021, as well as the updated BCBS POR that were published around the same time as mentioned earlier in this briefing.

Beyond policy setting, the effective implementation of operational resilience requires a collaborative approach involving both the public and private sectors to establish common guidelines, standards and solutions. The primary vehicle for such collaboration in the UK is the Cross Market Operational Resilience Group (CMORG) which is co-chaired by the Bank of England and the UK Finance. J.P. Morgan is a standing member of CMORG and co-chairs a number of the CMORG sub-groups including the Chief Information Officers' Forum and the Sector Exercise Group.

J.P. Morgan is also actively participating in the market-wide and industry-sponsored resilience testing exercises – for example, the annual SIFMA resilience test for member firms and key FMIs in the US and the Sector Simulation Exercise

(SIMEX) in the UK, which was last hosted in 2018 and is next planned for the fourth quarter of 2022.

In the context of our engagement on cybersecurity at an industry level, J.P. Morgan is a leader in the Financial Services Information Sharing & Analysis Center (FS-ISAC), which is an intelligence-sharing cooperative for the financial services sector. In the US, our firm has also helped to drive the creation of the Analysis and Resilience Center (ARC) for Systemic Risk, which is an industry-funded non-profit organization whose mission is to increase the resilience of the systems that underpin the US financial services sector. J.P. Morgan is also a leader in the Cyber Risk Institute (CRI), a non-profit industry coalition that promotes enhancing cybersecurity and resilience through standardization. The CRI maintains the Cybersecurity Profile (FSP) tool used by firms to benchmark their cybersecurity and resilience capabilities.

Close focus by the regulators and the financial services industry on operational resilience is here to stay for the foreseeable future given the evolving cyber risk landscape, geopolitical environment, pace of innovation and technological development and climate change. J.P. Morgan will continue to monitor and engage in the regulatory landscape on operational resilience as well as collaborate with the governments, regulators, peers in the marketplace, clients, FMIs and third-party vendors to ensure that we as a firm, and the wider industry, are coordinated in the collective effort to evolve and enhance operational resilience best practices and frameworks.

Contributors

Operational Resilience – Global Regulatory Developments and J.P. Morgan Industry Engagement

Matthew Field	J.P. Morgan Cyber and Technology Policy and Partnerships
Janice Fernandes	J.P. Morgan Securities Services – Global Regulatory Practice
Andrew Morris	J.P. Morgan Corporate & Investment Bank Business Resiliency
Michael Mykytiw	J.P. Morgan Securities Services – Global Regulatory Practice
Jack Parker	J.P. Morgan Securities Services Industry Developments
Julia Stepanian	J.P. Morgan Securities Services – Global Regulatory Practice
Lindy Vannavong	J.P. Morgan Securities Services – Global Regulatory Practice

For additional information, please contact your J.P. Morgan representative.