Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic & lessons for future disruptions

Final Report

The Board
OF THE
INTERNATIONAL ORGANIZATION OF SECURITIES COMMISSIONS

FR06/22	**JULY 2022**

Copies of publications are available from:
The International Organization of Securities Commissions website www.iosco.org

Contents

EXECUTIVE SUMMARY

The ongoing COVID-19 pandemic (pandemic) and the response of governments, markets and entities, has tested the operational resilience of the global market system like never before. The extensive concerns, limitations or restrictions on mobility and business operations experienced around the world have challenged supply chains, fragmented workforces, and created barriers between regulated entities and employees and their clients and counterparts. The pandemic stretched crisis management, business continuity, disaster recovery and supplier management arrangements and, in some cases, and to varying degrees, these challenges remain.

Trading Venues[1] and Market Intermediaries[2] (together 'regulated entities') have to date largely proved to be operationally resilient during the pandemic. They have served their clients and the broader economy, despite periods of extreme market volatility and record trading volumes. This is a testament to the work done on operational resilience over the last decade. The pandemic has, however, also highlighted opportunities to further improve regulated entities' operational resilience.

IOSCO published a Consultation Report[3] on 13 January 2022 which examined the operational resilience of regulated entities during the pandemic as well as existing IOSCO and other international organizations' principles and guidance on operational resilience.[4] The majority of responses to the Consultation Report agreed with the observations identified in the Consultation Report and supported the lessons learned. In particular, respondents welcomed alignment of definitions with existing IOSCO and other international organizations' principles and guidance on operational resilience to help to ensure consistent standards. Respondents also provided other examples of impacts, risks challenges and lessons learned during the pandemic. IOSCO has considered all the feedback and integrated this into the Report.

Even though this report is focused on risks, challenges and lessons learnt during the pandemic, challenges to operational resilience can arise from a range of other possible disruption scenarios.

---

1 A Trading Venue encompasses exchanges or other multi-lateral trading facilities, including, for example, alternative trading systems and multi-lateral trading facilities (MTFs). It also refers to the operator of a particular exchange or trading facility. A Trading Venue does not, however, include a single dealer system or a broker crossing facility.

2 Market intermediaries generally include those who are in the business of managing individual portfolios, executing orders and dealing in, or distributing, securities. Market intermediaries generally include "investment advisers", which are those principally engaged in the business of advising others regarding the value of securities or the advisability of investing in, purchasing or selling securities.

3 IOSCO CR01/22 *Operational resilience of trading venues and market intermediaries during the COVID-19 pandemic* (2022) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD694.pdf

4 While this report relates to trading venues and market intermediaries, the lessons may also be relevant to other entities, including financial market infrastructure providers.

This Report:

- summarizes some of the existing operational resilience work by IOSCO and other international organizations;
- outlines how the pandemic impacted regulated entities;
- examines the key operational risks and challenges that regulated entities faced during the pandemic. In particular, the rapid and widespread shift to remote working, the subsequent rise of hybrid working in many jurisdictions and increased reliance on IT systems. The pandemic also increased cyber security risks, accelerated the adoption and use of existing, new and emerging technologies and created disruptions to arrangements with third parties; and
- builds on existing IOSCO and other international organizations' principles and guidance on operational resilience by providing additional observations and identifying lessons learned from the pandemic. This should inform regulated entities' future operational resilience arrangements.

Summary of key lessons learned on operational resilience during the pandemic

The existing IOSCO principles, recommendations and guidance relating to operational resilience provide the core structure for regulated entities and regulators when considering operational resilience. The following lessons from the pandemic may be useful to help enhance their operational resilience:

A. **Operational resilience means more than just technological solutions** – the operational resilience of a regulated entity depends as much on the regulated entity's processes, premises and personnel as its technology when faced with a significant disruption.

B. **Consider dependencies and interconnectivity** – full business processes and all dependencies and interconnections are important to consider before and after a disruption to adequately assess potential risks and changes to controls. Critical to this is consideration of the role of service providers and off-shore services, whether intra-group or third parties.

C. **Review, update and test business continuity plans (BCP)** – BCP (including scenario planning) are important to review and consider whether updates are appropriate to reflect lessons learned from the pandemic. For example, pre-pandemic operations may not be restored for a prolonged period, a disruption may impact all or multiple locations at the same time and a broad range of scenarios (even those that are unlikely) may be appropriate to be tested. The pandemic highlighted the importance of communication channels between regulators, key authorities, regulated entities, and third-party service providers to help understand any impacts on operational resilience.

D. **Effective governance frameworks** – the pandemic highlighted the importance of an entity's effective governance framework to facilitate and support operational resilience due to potentially novel and fast-paced situations or changes that might arise. Decisions made under pressure may need to be revisited and tested if they impact the business beyond the period of disruption.

E. **Compliance and supervisory processes** – greater automation and less dependence on physical documents and manual processes by regulated entities may better accommodate a remote workforce. A review of monitoring and supervision arrangements by regulated entities for remote workforces may be appropriate to help ensure continued effectiveness in a remote or hybrid environment.

F. **Information security risk** – decentralized and remote work may increase the importance of monitoring processes to help ensure information security, and in particular, to prevent cyber-attacks.

Chapter 1 - Background to Operational Resilience

Maintaining and enhancing the operational resilience of the financial sector and regulated entities is a long-standing regulatory priority.

(a) What is operational resilience?

For the purposes of this Report, operational resilience refers to the ability of a regulated entity to deliver critical operations through disruption. This ability enables a regulated entity to identify and protect itself from threats and potential failures, respond and adapt to, as well as recover and learn from, disruptive events to minimize their impact on the delivery of critical operations through disruption.

This description of operational resilience is based on the definition of operational resilience used by the Basel Committee on Banking Supervision (BCBS) in its *Principles for Operational Resilience.*[5] For the purposes of this Report, IOSCO considers there is merit in aligning the definition of operational resilience for trading venues and market intermediaries with that of the BCBS. This may encourage consistency among regulatory frameworks of, or to be developed by, national competent authorities that regulate both entities. A consistent definition may also assist organizations that operate a entities across different financial services, such as stockbroking and retail banking, that are subject to different regulatory regimes. It should be noted, however, that specific policies and procedures of operational resilience for trading venues and market intermediaries may differ from that of a bank.

An operationally resilient regulated entity is less prone to incur lapses in its operations and losses from disruptions. This should lessen the impact of an incident on critical operations and related functions, services and systems as well as the impact on the market participants that the entity serves and markets in which it operates. A regulated entity's level of operation resilience will also depend on its risk appetite and tolerance for disruptions to critcial services following a disruption.

(b) What are critical operations?

Operational resilience requires extensive planning and preparation, including the identification of a regulated entity's critical operations, relationships and activities and consideration of the possible risks to its ability to deliver its critical operations. Critical operations encompass critical functions.[6] It also includes the consideration of the potential steps that can be taken to prevent or mitigate risks that may create disruption, how to respond and how to recover critical operations when a disruption occurs.

---

5 BCBS *Principles for Operational Resilience* (2021) https://www.bis.org/bcbs/publ/d516.pdf

6 Critical functions will vary based on trading venues' and market intermediaries' activities. For context, the FSB considers critical functions for banks as activities performed for third parties where failure would lead to the disruption of services that are vital for the functioning of the real economy and for financial stability due to the banking group's size or market share, external and internal interconnectedness, complexity and cross-border activities. Examples include payments, custody, certain lending and deposit-taking activities in the commercial or retail sector, clearing and settling, limited segments of wholesale markets, market-making in certain securities and highly concentrated specialist lending sectors. *FSB Recovery and Resolution Planning for SIFI* (2013) https://www.fsb.org/wp-content/uploads/r_130716a.pdf

Critical operations include activities, processes, services and their relevant supporting assets[7], the disruption of which would be material to the continued operation of the regulated entity. Whether a particular operation is "critical" depends on the nature of the regulated entity and its role in the financial system.

As with the description of operational resilience, IOSCO is drawing on the BCBS's description of critical operations.[8] However, again, while the underlying principles may be the same, the specifically identified critical operations of a regulated entity may differ from that of a bank.

Further, the identification of the critical operations of a regulated entity may vary depending on the nature of the entity and may include the products and services provided, the client base, regulatory requirements and the wider group structure of the entity.

For a regulated entity, critical operations may include activities such as, but not limited to:

- access to services for clients or participants;
- accepting orders and executing trades for clients or participants in agreed asset classes during trading hours;
- efficient and accurate documentation and record keeping requirements;
- providing and meeting settlement and clearing processes and requirements;
- ability to facilitate capital raising services, as appropriate; and
- where appropriate, the ability to transfer trading to other trading venues if there is a system outage or other possible failures.

For trading venues, these may include systems and processes relating to order entry, order routing execution systems, data dissemination, network infrastructure, market regulation, risk management systems, surveillance and the like to help ensure critical operations are provided.[9]

For market intermediaries, there is more diversity in what the critical operations may be, again depending on the nature of the products and services being provided, the client base and regulatory requirements (e.g., a market maker has some very different critical operations compared to a retail stockbroker).

(c) Existing IOSCO work on operational resilience

In previous reports, IOSCO considered the operational resilience of regulated entities from the perspective of the resilience of critical systems (i.e., business functions and systems that are critical to continue operations).[10] The concept of operational resilience, however, is broader than systems and refers to the ability of a firm to help ensure the continuity of the provision of

---

7 As defined by BCBS: in this context, "*supporting assets*" are defined as people, technology, information and facilities necessary for the delivery of critical operations. BCBS *Principles for Operational Resilience* (2021) See: https://www.bis.org/bcbs/publ/d516.pdf

8 Id.

9 List from the Committee 2 Report, infra note 6.

10 The Committee 2 Report defined *critical systems* for purposes of that report as "*all computer, network, electronic, and technological systems that directly support trading operated by or on behalf of the applicable Trading Venue, including order routing, market data, market regulation, or market surveillance*."

financial services through any disruption and, in particular, identify threats, respond and adapt to them and recover and learn from a disruptive event.[11]

The most relevant IOSCO reports that consider operational resilience (the IOSCO Reports) include the following:

- Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (2015) (Committee 2 Report);[12]
- Market Intermediary Business Continuity and Recovery Planning (2015) (Committee 3 Report);[13]
- Committee on Payments and Market Infrastructures (CPMI) and IOSCO (CPMI-IOSCO) Level 3 assessment of FMIs' business continuity planning; [14]
- CPMI-IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures (2016) (Cyber Resilience Report); [15]
- IOSCO Principles on Outsourcing Report (2021) (IOSCO Outsourcing Report).[16]

The Committee 2 Report and Committee 3 Report

The Committee 2 Report and Committee 3 Report discuss a number of operational resilience topics that are useful for regulated entities during the pandemic, including:

- the **management of technology to mitigate risk**, with a focus on key areas to facilitate resilient systems critical to the operations of trading venues. These include governance, resources, ongoing monitoring of systems, incident management, change management, cyber security and resilience and outsourcing; and
- key aspects of **business continuity planning**, including scenario testing, governance, the role of senior management and critical personnel, minimum system service levels, back-up and system redundancy arrangements, communications (both internal and external), recordkeeping, testing and reviews of BCP and outsourcing.

---

11 There are also different definitions, see for example the BoE and the FCA definition, "operational resilience is the ability of firms and FMIs and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions" (bankofengland.co.uk) Bank of England, Building operational resilience: Impact tolerances for important business services (2019) https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/consultation-paper/2019/building-operational-resilience-impact-tolerances-for-important-business-services.pdf?la=en&hash=DAD20B3E08876E418863D37A242214BB1F32FE0A

12 IOSCO FR31/2015 *Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity* (2015) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD522.pdf

IOSCO FR32/2015 *Market Intermediary Business Continuity and Recovery Planning* (2015) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD523.pdf

CPMI-IOSCO *Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning* (2021) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD680.pdf

15 CPMI-IOSCO Guidance on cyber resilience for financial market infrastructures (2016) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD535.pdf

16 IOSCO FR07/2021 *Principles on Outsourcing* (2021) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD687.pdf

For **trading venues**, the Committee 2 Report includes sound practices to consider with respect to operational resilience, reliability, and integrity, including security of their critical systems, and sound practices to protect against external risks to critical systems posed by access to trading venues and by cyber-threats.

For **regulated entities**, the Committee 2 Report and Committee 3 Report also contain sound practices to consider when developing BCP, a key part of any operational resilience work.

For **regulators**, the Committee 2 Report and Committee 3 Report included recommendations and standards that may be relevant to operational resilience of regulated entities.

- From the Committee 2 Report:
    - Regulators should require trading venues to have in place mechanisms to help ensure the resilience, reliability, and integrity (including security) of critical systems; and
    - Regulators should require trading venues to establish, maintain, and implement BCP.

- From the Committee 3 Report:
    - Regulators should require market intermediaries to create and maintain a written BCP identifying procedures relating to an emergency or significant business disruption; and
    - Regulators should require market intermediaries to update their BCP in the event of any material change to operations, structure, business, or location and to conduct an annual review of it to determine whether any modifications are necessary in light of changes to the market intermediary's operations, structure, business, or location.

The Cyber Resilience Report covers sound cyber governance, threat intelligence and rigorous testing, culture of cyber risk awareness and the requirements in the wider ecosystem of an entity. These areas are important to be considered in any steps taken to ensure operational resilience.

The IOSCO Outsourcing Report outlines a number of principles in relation to outsourcing and specifically states:

> *"This [pandemic] and the greater reliance on outsourcing serve as a useful reminder to increase attention to operational resilience issues. Regulated entities should consider the Principles on Outsourcing when thinking about how to maintain and improve resilience. Regulated entities should consider the Principles on Outsourcing when thinking about how to maintain and improve resilience."*[17]

The principles relate to due diligence in the selection and monitoring of a service provider and a service provider's performance, the contract with a service provider, information security, BCP and disaster recovery, concentration risk, rights of inspection and termination. The IOSCO Outsourcing Report considered these principles in the context of the pandemic and

[17] Ibid. note 16.

identified some specific areas that were highlighted by the pandemic, including the impact of third- party service providers moving to remote work and increasing reliance on technology.

IOSCO notes that many regulators have focused their regulatory and supervisory programs on the operational resilience of operations and processes, in addition to focusing on information technology systems.[18] In IOSCO's view, our previous work on the resilience of critical systems and BCP continues to provide a strong foundation for considering the broader issues involved in developing operational resilience.

(d) Existing work on operational resilience from other organizations

IOSCO has also examined the work on operational resilience undertaken by other international organizations, regulators, and authorities, such as the BCBS,[19] the U.S. banking regulators, the Bank of England and the Financial Conduct Authority (FCA).

A range of other organizations have also produced materials on operational resilience that IOSCO considers important in respect to operational resilience, including:

- The "Risk Register" developed by the FICC Markets Standards Board (FMSB);[20]
- Joint work by the Global Financial Markets Association and Institute of International Finance;[21] and

---

18 E.g., Bank of England and Financial Conduct Authority, *Building The UK Financial Sector's Operational Resilience*" (2019), available at:

https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/discussion-paper/2018/dp118.pdf; European Commission, *Digital Operational Resilience Framework for Financial Services: Making the EU Financial Sector More Secure* (2019):

https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/2019-financial-services-digital-resilience-consultation-document_en.pdf

US FED-FDIC-OCC, *Sound Practices to Strengthen Operational Resilience* (2020) *Sound Practices to Strengthen Operational Resilience)* https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-144a.pdf; Monetary Authority of Singapore, *Ensuring Safe Management and Operational Resilience of the Financial Sector (mas.gov.sg)* (2020) https://www.mas.gov.sg/who-we-are/annual-reports/annual-report-2019-2020/mas-response-to-covid-19/ensuring-safe-management-and-operational-resilience-of-the-financial-sector

19 The BCBS Principles for Operational Resilience for banks (2021) see footnote 4. "*The resilience of banks and securities firms are mutually dependant, and many firms are subject to both prudential and securities regulation. The BCBS Principles cover governance, operational risk management, business continuity planning and testing, mapping interconnections and interdependencies, third party dependency management, incident management and ICT, including cyber security*".

20 See FMSB *Spotlight Review* and *Risk Register* available at: *FMSB Spotlight Review on examining remote working risks in FICC markets – FICC Markets Standards Board* (2021); https://fmsb.com/fmsb-publishes-spotlight-review-on-examining-remote-working-risks-in-ficc-markets / and *Examining-remote-working-risks-in-ficc-markets* (2021) https://fmsb.com/wp-content/uploads/2021/09/Spotlight-Review-%E2%80%98Hybrid-working-in-FICC-markets-%E2%80%93-Future-risk-management-frameworks-.pdf

21 IIF and GFMA *Priorities for Strengthening Global Operational Resilience Maturity in Financial Services* (2021) https://www.iif.com/Publications/ID/4257/Priorities-for-Sovid-19-pandemic-from-a-financial-stability-perspective-interim-report

- FSB's Lessons Learnt from the Pandemic from a Financial Stability Perspective.[22]

A summary of some of the conclusions from some of these reports is attached as **Appendix A**.

(e) Summary

The principles, recommendations and guidance set out above have provided a strong foundation for developing operational resilience. However, the unique experiences of the pandemic provide additional lessons and illustrative examples that may be beneficial for regulated entities in considering their operational resilience.

[22] FSB *Lessons learnt from the COVID-19 pandemic from a financial stability perspective: Final Report* (2021) https://www.fsb.org/wp-content/uploads/P281021-2.pdf

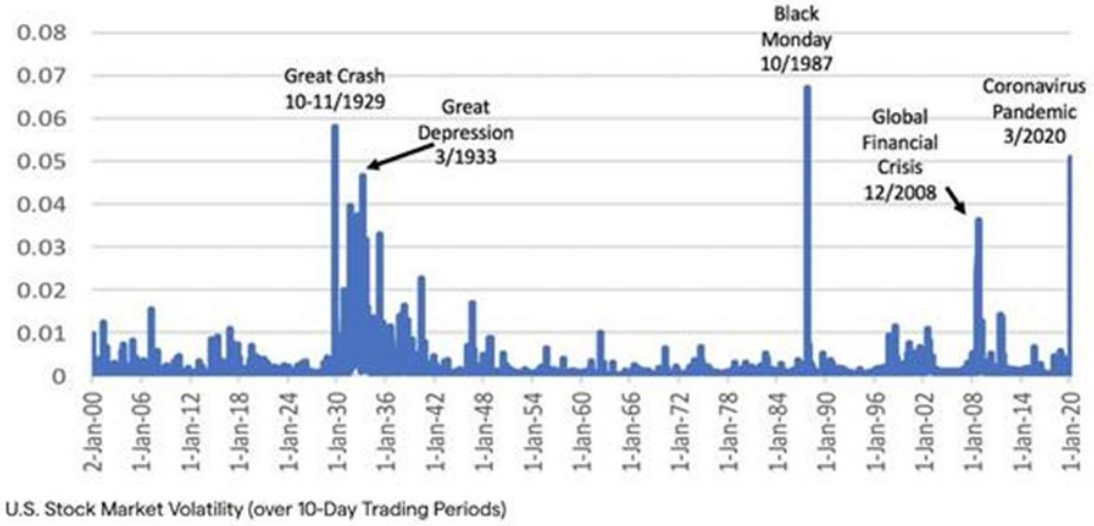
Chapter 2 - Market Volatility During The Pandemic

(a) Extreme market volatility

Early in the pandemic, there were periods of extreme price volatility and disruption to the operation of markets.

From mid-February until March 2020, prices in financial markets fell at one of the fastest paces in modern history. Major equity indices lost close to 40% in 20 days while volatility surged to the highest levels observed since the global financial crisis (GFC) in 2008/09. Stock prices fell as much in this 20-day period as they did in one year during the GFC. The rapid fall in the value of financial markets occurred across a range of asset classes, from equities to investment grade and high yield corporate bonds.[23]

Figure 1: US stock market volatility (over 10-day trading periods) – 1900 to 2020



Source: Farm Together, October 2020 "COVID-19's Unprecedented Impact on Stock Market Volatility".

Over the past decade, trading venues have invested significant resources into developing volatility control mechanisms that help to maintain fair and orderly markets during periods of extreme market volatility.[24] Trading venues have regularly tested their capacity to ensure that systems can be scaled for unexpected increases in trade messages. As a result, trading venues were largely able to manage and continue operations, with scalability, volatility mechanisms and circuit breakers largely working as designed. For example, in response to the extreme volatility, market-wide circuit breakers in the U.S. and Canada, working as designed, were tripped for the first time in 30 years and four times within an eight-day window. As Figure 1

---

23 ESA Joint Committee Report on *Risks and Vulnerabilities in the EU Financial System*, September 2020 (2020) https://www.esma.europa.eu/document/joint-esa-report-risks-and-vulnerabilities-in-eu-financial-system-2020

24 IOSCO *FR13/2018 Mechanisms Used by Trading Venues to Manage Extreme Volatility and Preserve Orderly Trading* (2018) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD607.pdf

illustrates, it was comparable to other major financial crises over the past 100 years, and in some cases more volatile.

In February-March 2020, some regulators and trading venues stepped in to reduce position limits across the market. For example, the Security and Exchange Board of India reduced position limits for stock and equity index derivatives, and increased the margin required in the cash market. It also required upfront collection of margins and restricted the use of powers of attorney. These measures were designed to ensure investors could meet their obligations in the fast-moving market.

(b) Amplified trading activity

In addition to periods of extreme price volatility, there were significant spikes in the number of orders and trades moving through the market system. Trading venues across equity and derivative exchange markets experienced around a 50% increase in trading in Q1 2020 compared to Q1 2019.[25]

Table 1: US exchange statistics Q1 2019 compared to Q1 2020

	Q1 2019	Q1 2020	% increase
Equity			
Value traded	31,759	46,214	46%
Electronic order book	23,850	35,181	48%
Derivatives			
# Contracts (m)	7,526	11,070	47%
Value (notional)	672,378	951,095	41%

Source: WFE data. Values are US$bn

In Australia, for example, the equity market experienced multiple consecutive days of record trade numbers in March 2020, peaking at double the previous high. This placed unprecedented strain on the trade processing capacity of the market infrastructure, as well as the middle and back offices of market intermediaries, causing delays in trade processing. To safeguard market resilience, the Australian Securities and Investments Commission issued temporary directions to the largest equity market intermediaries to limit the number of trades.[26]

The large trade numbers also tested the capacity of some market intermediaries and their ability to perform important services. For example, a broker-dealer in the United States experienced

---

25 ICI *The Impact of COVID-19 on Economies and Financial Markets* (2021) https://www.ici.org/system/files/private/2021-04/20_rpt_covid1.pdf

26 20-062MR *ASIC takes steps to ensure equity market resiliency* | ASIC - Australian Securities and Investments Commission (2020) https://asic.gov.au/about-asic/news-centre/find-a-media-release/2020-releases/20-062mr-asic-takes-steps-to-ensure-equity-market-resiliency/

service outages.[27] There are examples where other market intermediaries faced challenges in executing client orders.

Market intermediaries in many jurisdictions experienced large numbers of new investors opening accounts or existing investors reactivating their accounts. The surge in demand put considerable strain on onboarding teams and know your client / anti money laundering (KYC/AML) checks. This was particularly problematic for entities that relied on manual onboarding processes. The increased volumes resulted in longer lead times to open accounts, increased the workload for processing teams and created a pressured environment where mistakes may be more prevalent, or processes may be circumvented. In addition, technology was strained as some market intermediaries did not have the bandwidth to manage an increase in orders, requests or complaints from investors.

In the area of post-trade processing, many market intermediaries were operationally stretched, especially in cash equities and fixed income, and reported a considerable backlog of transactions to process and increased fail volumes in settlements, payments, and collateral-related processes. Settlement failures can create unmargined, counterparty risk. The Depositary Trust & Clearing Corporation (DTCC) issued a report based on its 2020/21 survey that 58% of sell-side firms reported challenges in settlement and payments during peak volatility in 2020.[28] Some regulated entities organized several weekend sessions to reduce backlogs.

Despite the challenges of increased volatility and volumes, the markets and regulated entities generally continued to operate in an orderly manner.

Risks to operational resilience

Volatile markets or increased trading activity may raise risks to operational resilience. If a trading venue's technology cannot manage increased messaging or volatility, trading may be disrupted and as a result, fair, orderly and efficient markets may be impacted. This may lead to investor losses or undermine confidence in markets. If market intermediaries' systems cannot handle increases in order or trading volumes, account openings or volatile markets, it may also lead to investor losses or reduced confidence in markets.

---

27 *FINRA Orders Record Financial Penalties Against Robinhood Financial LLC* | FINRA.org (2021) https://www.finra.org/media-center/newsreleases/2021/finra-orders-record-financial-penalties-against-robinhood-financial

28 DTCC White Paper, Managing-Through-a-Pandemic-Covid19-Whiteaper (2021) https://www.dtcc.com/-/media/Files/Downloads/WhitePapers/Managing-Through-a-Pandemic-Covid19-Whiteaper.pdf

Chapter 3 - Operational Resilience During The Pandemic

The pandemic has posed the first large scale test to the global financial sector since the implementation of the GFC reforms. Enhancements to operational resilience were incorporated as a result and, in some areas, increasing reliance on technology has helped to increase resilience.

In addition to managing the challenges of heightened market volatility and trading activity (see Chapter 2 above), regulated entities adapted quickly to the sudden move to remote working early in the pandemic. They utilized technology, including new forms of communication, to facilitate remote working and provide continuity of service. Critical operations continued to be delivered as regulated entities:

- rapidly deployed and adapted their BCP to ensure that their critical operations continued to be provided;
- separated their workforces into groups to work from different locations or on different days to minimize the risk of the spread of COVID-19;
- rapidly adopted new technology products and systems, including acquiring additional equipment and using of video conference platforms to ensure staff could continue to engage with one another, clients and other stakeholders;
- worked closely with industry bodies, governments and regulators to identify challenges, areas where relief was required from certain regulatory/legal obligations and the wider need for regulated entities to continue to operate in trying times; and
- on-shored a range of operations as some off-shore providers experienced difficulties in continuing to provide services in a remote working model.

In many instances, regulated entities implemented or accelerated the implementation of changes to their operations, including to the mobility of their workforce and adopting technology that might otherwise have taken years to implement.

As outbreaks of COVID-19 (and its variants) continue, remote working or hybrid working models have been extended and the approaches to returning to the office have been varied, and frequently deferred. Regulated entities have also had to adapt their business models, including how services are delivered, monitored and supervised in a remote work environment.

Despite the significant changes to working arrangements, including the increased adoption of digital solutions, very few incidents of significant disruption or issues (such as misuse of confidential information) have been reported or detected to date. IT systems have been remarkably resilient throughout the pandemic, with few major outages reported. Capital markets have also continued to function efficiently with significant equity and debt raisings and elevated levels of mergers and acquisition activity.

(a) Regulated entities were generally well prepared

The work of regulators and regulated entities on operational resilience, particularly after the GFC, meant they were considered to be well prepared for the disruption that the pandemic and the limitations and other responses created, even though the extent of the disruption may not have been anticipated.

Based on information gathered by IOSCO, key measures that helped regulated entities remain operationally resilient included effective BCP, cyber resilience, information security, robust and scalable systems, volatility control mechanisms, and the implementation of effective and robust governance arrangements that helped regulated entities quickly adjust their business operations to the reality of the pandemic.

Most of these measures reflect the recommendations or practices identified in the Committee 2 Report and Committee 3 Report. This was confirmed in IOSCO's Assessment Committee Report *Thematic Review on Business Continuity Plans with respect to Trading Venues and Intermediaries.* This report found that "on balance trading venues and market intermediaries seem to have been resilient, from an operational point of view, during the initial and subsequent phases of the pandemic, and seem to have functioned largely as designed."[29]

The DTCC report M*anaging through a Pandemic: The Impact of COVID-19 on Capital Markets Operations*[30] also noted that, as a result of preparations, market intermediaries in the US were able to react quickly and effectively to the pandemic due to the "…significant investments made in scaling, automating, and upgrading core operations and capital markets infrastructure over the past several years, as well as the significant BCP tests they have encountered in the past…" market intermediaries viewed their "…ability to withstand the spikes in trade volumes as validating their investments in BCP preparedness and in putting in place a scalable infrastructure through significant multi-year transformation programs."

(b) Regulators responded in a timely and proportionate manner

Many regulators acted early in the pandemic to facilitate fair and orderly markets, and some provided relief to regulated entities from various regulatory obligations on a temporary basis. For example, some regulators provided relief from requiring wet signatures, in-person meetings, some elements of telephone recording requirements, and the timelines for regulatory reporting[31]. Some regulators also delayed the introduction of new regulations,[32] while others accelerated regulation relating to digital operational resilience.[33] In addition, some regulators delayed on-site inspections of regulated entities.

---

29 IOSCO FR03/2021 *Thematic Review on Business Continuity Plans with respect to Trading Venues and Intermediaries* (2021) https://www.iosco.org/library/pubdocs/pdf/IOSCOPD675.pdf

30 DTCC Report, Ibid.

31 FINRA's Frequently Asked Questions Related to Regulatory Relief Due to the Coronavirus Pandemic FINRA.org; SEC adopts rules to facilitate electronic submission of documents: SEC.gov | SEC Adopts Rules to Facilitate Electronic Submission of Documents to the Agency and SEC.gov | Staff Statement Regarding Rule 302(b) of Regulation S-T in Light of COVID-19 Concerns; ASIC grants relief to industry to provide affordable and timely financial advice during the COVID-19 pandemic: 20-085MR ASIC grants relief to industry to provide affordable and timely financial advice during the COVID-19 pandemic | ASIC - Australian Securities and Investments Commission and 20-068MR Guidelines for meeting upcoming AGM and financial reporting requirements | ASIC - Australian Securities and Investments Commission; and *CFTC provides temporary, targeted relief to market participants in response to COVID-19*: Coronavirus | CFTC .

32 For instance, ASIC deferred publication of final report on changes to its market integrity rules.

33 Proposal for a Regulation of The European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 published on 24 September 2020, EUR-Lex - 52020PC0595 - EN - EUR-Lex https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0595

Regulators also sought to provide timely feedback on the evolving situation and guidance to regulated entities on issues to consider and lessons being learnt from other stakeholders or from other jurisdictions. In addition, many regulators increased the frequency of communication with regulated entities at the beginning of the pandemic, as the entities shifted their processes and operations to a remote environment.

Chapter 4 - Risks and Challenges of The Pandemic

The pandemic provided a real-life examination of regulated entities' operational resilience and the evidence seems to be that regulated entities subject to the regulation of IOSCO member jurisdiction authorities were largely resilient. IOSCO is of the view that the previous IOSCO work, as reviewed above, continues to provide a robust core structure for regulated entities and regulators when considering operational resilience.

However, in reviewing the impact of the pandemic on regulated entities, IOSCO has identified some unique operational resilience challenges, risks, and lessons learned that could be used to supplement the recommendations and sound practices in the Committee 2 Report and the standards, guidance and sound practices in the Committee 3 Report. The lessons are relevant to other possible disruption scenarios, and not just pandemics.

This section examines some of the key risks and challenges to operational resilience that may have arisen due to the pandemic (including, risks relating to the shift to remote working, cyber security risk, increased reliance on IT systems, new and emerging technologies and the use of third parties). It also notes that some of the fundamental changes that may have occurred early in the pandemic, and which could impact a regulated entity's operational resilience, may become permanent as a result of changes to the operations of regulated entities. Regulated entities should consider taking these risks into account as they evaluate their policies and procedures on operational resilience and, if appropriate, think about how to mitigate them adequately.

Based on the experiences of IOSCO members, many of the challenges to operational resilience were common across jurisdictions. Some differences did emerge in the extent to which regulated entities were prepared for remote working and their level of technological preparedness. For example, some regulated entities had already moved to online service and cashless service provision and addressed issues associated with these changes. However, for jurisdictions that were heavily reliant on in-person meetings, paper documentation and/or the use of cash, the rapid lockdowns implemented in response to the pandemic created challenges. This was exacerbated if some people did not have access to or were not proficient in the use of IT systems. The experiences described in this section may not have been experienced by all regulated entities or in all jurisdictions but provide a picture of some of the different challenges faced.

In general, it is important that regulated entities also understand that these pandemic related and some other operational resilience challenges may continue to be symmetrical and may occur again in the future; that is challenges that impact all regulated entities almost equally rather than just a specific entity or subset of entities. Typically, operational resilience has been considered an asymmetrical challenge where only one regulated entity or service provider experienced a disruption to their services. Together with its global impact, the pandemic has therefore identified a new level of symmetrical risk to operational resilience that may not have been anticipated previously.

(a) Sudden and sustained shift to remote working

Based on the experiences of IOSCO members, it appears that many regulated entities' BCP may not have anticipated a scenario where the lack of access to primary sites would occur at

the same time as the secondary or back up sites were also unavailable for a prolonged period. As a result, during the early days of the pandemic, regulated entities had to quickly redeploy staff to work from home.[34]

In some jurisdictions, there were supply shortages of hardware (e.g., computer monitors, keyboards, mobile phones, desks and chairs) and system limitations with licenses allowing remote access. Many regulated entities improvised by lending staff equipment from the office or allowing staff to use personal computers to establish home offices. These issues were quickly resolved and seemed to have minimal impact on the ability of regulated entities to perform their critical functions. In addition, there were some intermittent disruptions to remote working during the pandemic which impacted the productivity of staff working from home, for example, local power and internet outages.

Many regulated entities embarked on a speedy roll-out of new or expanded forms of communication (i.e., video conferencing), collaboration and staff monitoring software. However, with the rapid adoption of this technology, the usual IT security checks may have been bypassed in the haste for access, posing increased risks. For example, there were wide-spread reports of security issues with one video conferencing provider.[35] Over time, however, entities reviewed video conference arrangements and added additional protections or changed providers.

Some market intermediaries experienced issues with managing client communications, with lockdowns preventing access to call centers or third-party service providers. Limited bandwidth of home internet connections amplified this issue in some cases.

Some adjustments to working arrangements were necessary for trading venues in March 2020. Trading venues that use open outcry quickly implemented plans to conduct trading electronically. For example, the New York Stock Exchange closed its trading floor for two months and converted to fully electronic trading to comply with the state of New York's stay-at-home order. In addition, the London Metals Exchange ring moved to electronic trading in March 2020, but in-person trading resumed in September 2021.

In a few other jurisdictions, some trading venues were required to shut or otherwise reduce activity at the start of the pandemic. Often closures were the result of the pandemic and responses that included broader, business or national restrictions or curfew measures and not due to technological issues or business continuity planning failures.

Risks to operational resilience

The speed at which the pandemic and related limitations or jurisdictional restrictions impacted regulated entities meant that decisions about operations and the ability to operate had to be made quickly. This highlighted the importance of a strong governance framework to enable

---

[34] For instance, the NFA noted many of its members' business continuity disaster recovery (BCDR) plans assumed that their back-up location would be accessible. In March 2020, the NFA issued a Notice to Members I-20-10 to ensure its members' BCDR plans considered the special circumstances of a pandemic. See News & Notices https://www.nfa.futures.org/news/newsNotice.asp?ArticleID=5208

[35] For example, *Zoom's Security Nightmare Just Got Worse: But Here's The Reality (forbes.com)* and *Zoom boss apologises for security issues and promises fixes - BBC News* (2020) https://www.bbc.com/news/technology-52133349

clear decision-making processes. Without such a framework, regulated entities may have been subject to delayed decision making which may have impacted operational resilience. Key decisions about operations were made quickly and often under pressure. These may have been based on incomplete information or with limited due diligence and could have tested an entity's risk tolerance. As the initial rush to make changes to operations subsides, regulated entities may need to back test these decisions to ensure they continue to be fit for purpose and are within their risk appetite.

Remote working and the use of personal equipment increases risks to information security, including cyber security and maintaining confidentiality. Prior to the beginning of the pandemic, in many regulated entities, few staff may have worked from home. This may have been as a result of business expectations, their preferences or the work culture, the design of control environments, limitations on systems and technology or regulatory expectations.[36]

Remote working arrangements for staff may have increased risk of unauthorized persons gaining access to information about clients, transactions, or trading. The risk to maintaining the confidentiality of information arises because of the lack of dedicated secure areas or where remote workspaces or computers are accessible to unauthorized persons. In addition, employees in remote work environments may be more exposed and less sensitized to risks of malicious software, social engineering or phishing attacks.

Figure 2 shows that the number of cyber-attacks increased significantly during the pandemic.[37] When there are significant disruptions that impact operational resilience this may increase the frequency of cyber-attacks. For example, these events may increase cyber vulnerabilities and the impact of a successful cyber-attack may be magnified. The technology used to facilitate remote working, or the use of personal devices may increase the risk of a cyber-attack, which could result in the disclosure of confidential information or could impact the operations of regulated entities. These risks may be heightened by the decentralized nature of access to systems and networks, the slow adoption of VPNs or the rapid adoption of software that may not have been adequately tested or configured. A lack of focus on these issues is more likely to impact a regulated entity utilizing remote working where there is more reliance on telecommunication technology and less on in-person interactions.

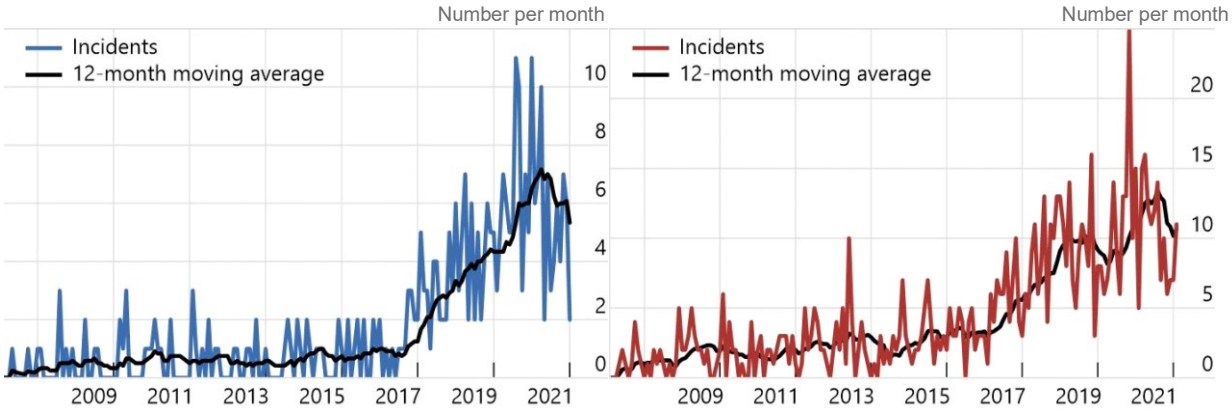
---

36 Ibid 19.

37 According to the FSB (*Lessons learnt from the COVID-19 pandemic from a financial stability perspective: Final report*): "The number of cyber attacks has increased significantly". Also, according to the ESMA *Report on Trends, Risks and Vulnerabilities of 2021*: "*for what concerns the financial sector more broadly, anecdotal evidence suggest that the number of cyber-attacks and scams has increased in the wake of the pandemic and technological transformation*," https://www.esma.europa.eu/sites/default/files/library/esma50-165-1842_trv2-2021.pdf

Figure 2: Cyber-attacks have become more frequent

1. Cyber incidents targeting financial institutions[1] 2. Significant cyber incidents[2]



[1] Panel 1 shows cyber incidents targeting financial institutions (including FinTechs) that are included in the Carnegie Endowment timeline. The timeline does not aim to capture every single incident, but to provide an insight into key trends. [2] Panel 2 shows significant cyber incidents recorded by the Center for Strategic & International Studies. These are defined as an economic crime with a loss of more than $1 mn, or an attack on government agencies, defence firms or technology companies.

Sources: Carnegie Endowment for International Peace; Center for Strategic & International Studies; FSB calculations.

In addition, remote working may heighten risks to information security. For example, the potential of staff emailing confidential material to personal email accounts, or printing confidential documents outside of the office, or from information being inadvertently seen or heard by unauthorized persons living in, or visiting, remote workspaces. These all increase vulnerabilities to cyber-incidents.

In some offices, compliance staff may have been physically near front office staff, which can facilitate engagement with the front line, thereby making oversight easier and more effective. This proximity is lost when staff are working from home. However, this risk does not always arise, because many regulated entities, have long relied on technology as a critical part of their compliance and surveillance activities.

In addition, a number of regulated entities rely on technology to monitor voice and electronic communications to supplement the work of compliance teams. Remote working may, however, make record keeping and reporting obligations more difficult. For example, the use of personal mobile phones for taking client orders can result in such calls not being captured on taped lines or records of communications not being made contemporaneously. Some loss of telephone recording and note taking may pose monitoring and supervision challenges for compliance staff. Remote working may also impact client communications and the proper handling of customer complaints in certain jurisdictions.[38]

There may, however, be some benefits to operational resilience from staff working remotely. This could include retention of knowledgeable staff who value the flexibility that remote

[38] IOSCO Retail Market Conduct Task Force, FR13/2020 I*nitial Findings and Observations About the Impact of COVID-19 on Retail Market Conduc*t, December 2020, (2020) available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD669.pdf

working provides, improved wellbeing and more robust business continuity planning (for instance not having to rely on secondary sites).

(b) Workforce challenges

For those regulated entities that retained a physical workforce in primary or back-up office locations, there were challenges in keeping those environments safe. Due to the pandemic risks, many governments imposed restrictions on entering restricted zones without relevant permits, rules around social distancing, mandatory mask wearing and limits on numbers of people in elevators, public transit, and other confined spaces. Additional requirements for specialized deep cleaning of workspaces were also imposed. Some businesses have imposed their own restrictions or continued restrictions for the same reasons.

As the pandemic continued, the shift to remote work raised additional workforce challenges. Prolonged remote working raised challenges for on-boarding new staff including delivery of electronic devices, training and embedding the desired work ethic and culture.[39] In addition, school closures necessitated home schooling for children of many employees, which divided workday focus.

Moreover, efforts to maintain the health, safety and well-being of staff became even more of a focus for many, as regulated entity employees worked longer hours and risked being overwhelmed or burned out.

Risks to Operational Resilience

The shift to remote work has the potential to hinder or stop employees from carrying out their functions. This may be caused by a lack of planning for off-site work or some of the technology-specific risks identified above.

In addition, the well-being of a regulated entity's workforce should always be of paramount concern, outside of its impact on the operations of the regulated entity. However, in the context of the pandemic, the impact of the pandemic, restrictions and remote working on staff created challenges to operational resilience.

Concerns were raised by some of those reviewed by IOSCO that a lack of staff engagement or focus could lead to ineffective decision-making, which could impact the services being provided to investors or participants. There may also be occupational health and safety implications if a workforce is at home for an extended period. A lack of engagement or burnout may lead employees to take medical leave or withdraw from employment. This could impact staffing levels, the ability of regulated entities to perform all functions, succession planning, or organizational knowledge. In addition, short or longer-term health issues may arise if employees' home office setups are not ergonomic.

[39] Joint paper issued by the Monetary Authority of Singapore and The Association of Banks in Singapore, *Managing the risks of remote working in financial institutions,* March 2021, (2021) available at: https://www.mas.gov.sg/news/media-releases/2021/managing-the-risks-of-remote-working-in-financial-institutions

(c) Shift to online, automated service provision

The shift of the bulk of operations to a virtual environment raised several practical issues for regulated entities and their participants, counterparts, or customers.

The shift to on-line service provision caused some trading venues to change their mechanism for facilitating trading. In particular, the physical floors of some trading venues were shut down for a period and they developed or implemented other mechanisms to allow for continued trading. For example, the Nigerian Exchange Group (NGX) provided advice and technical support for remote access to members that had previously relied on physical presence at exchanges and paper-based systems.

The pandemic and the limitations it brought, coupled with, restrictions and stay-at-home orders caused market intermediaries to quickly shift to increased reliance on technology. Guidance was provided, for instance, on how to hold effective meetings online that had previously been in person. Paper documentation was replaced with on-line documents and new mechanisms considered to help ensure compliance. In jurisdictions that had been more paper based, there was also a significant move to digitalization.

In some jurisdictions, regulators provided relief from legal and policy requirements to allow for virtual meetings and delayed compliance filings, and from wet signature requirements to allow for electronic signatures. In addition, the inability to rely on or use cash hindered client's and regulated entities' access to services.

Some examples of specific steps taken by regulators include:

- In Canada, IIROC provided relief to allow a written record of a client's instructions as an alternative to obtaining a client signature where a client does not have the capability to provide an electronic signature and for safety reasons does not want to be physically present to provide a wet signature; and
- The Nigerian Stock Exchange offered certain services to brokers that had previously traded on floor to allow them to continue to trade.

When the provision of services moved on-line, some organizations (e.g., IIROC) noted service level differences between clients who were technologically sophisticated and those who were not. This service gap meant that some less technologically sophisticated clients could not access their accounts or obtain services that were being provided electronically. This increased the burden on call centers, which were often not equipped to manage the volume of calls due to, among other things, a lack of personnel answering calls, either due to pre-pandemic operational or business decisions or due to pandemic effects, including restrictions.

Risks to operational resilience

Where paper communications cannot be delivered to clients who have difficulty receiving electronic communications, there is a risk that clients may not be able to obtain information that they need to make investment decisions, and a risk that clients may not be able to check confirmations of transactions for errors.

(d) Impact on outsourced and offshore third-party service providers

The pandemic exposed potential risks and vulnerabilities for businesses with outsourced or third-party operations. Many BCPs developed by regulated entities may have contemplated failures or issues with a single or a few outsourced service providers (whether at an affiliate or a third-party entity). They may not, however, have anticipated the possibility that all providers would face similar challenges at the same time or the implications of prolonged duration. Regulated entities have had to rely on third parties' recovery plans and assess what level of information they need in order to be reasonably comfortable with reliance on those plans.

In some jurisdictions, financial services (or their critical ancillary services) were not initially recognized as essential services. This meant that some providers of offshore services, including call centers, IT services and back-office processing functions, were unable to meet their service commitments due to jurisdictional restrictions on non-essential services with respect to office access, the inability or unsuitability of employees working from home or due to changes in operations or an increase in the volume of activity which extended processing times. In some instances, these offshore services were quickly brought onshore to the regulated entity's home country and resources were redeployed from other functions or new staff was hired.

In the context of local restrictions, relevant industry participants were active in encouraging governments with jurisdiction overseeing offshore service providers to designate key operational functions as essential services, such as "IT personnel managing data center operations and those responding to cyber events for critical infrastructure, third-parties supporting financial transactions and services, and workers supporting communications systems."[40]

According to the DTCC, 50% of firms reported at least some vendor disruption, and "not all firms had a robust contingency plan in place with their providers." That said, DTCC reported that over 90% of participants reported high levels of satisfaction with third-party providers and just a handful of the firms that were surveyed had to take processes back in-house.[41]

Important support services such as the printing and mailing of client communications and trade confirmations were also impacted by the restrictions. In many jurisdictions, regulated entities were able to move printed materials on-line and move from paper to electronic delivery.

However, it should also be noted that outsourcing to third-party providers, such as cloud services, may have enhanced operational resilience at financial institutions. This may be particularly the case in a number of emerging market and developing economies with less developed IT infrastructures, even if this gave rise to some of the challenges discussed above.[42]

Risks to operational resilience

---

40 SIFMA COVID-19: *Initial Lessons Learned and Considerations for Managing a Pandemic* (2020) https://www.sifma.org/wp-content/uploads/2020/10/SIFMA_COVID_19_Initial_Lessons_Report-101620L.pdf

41 *DTCC Managing through a pandemic: The impact of Covid-19 on capital markets operations* (2021). See footnote 28.

42 *FSB Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective*, see Footnote 22.

Consistent with the IOSCO paper entitled *Principles of Outsourcing*, the risks that exist with respect to outsourcing to a third-party service provider may be exacerbated by the impact of the pandemic and become more difficult to monitor.[43] They may be also exacerbated in other situations such as environmental or geo-political events.

If a regulated entity does not assess its interconnections and dependencies, or the operations of its service providers and the service provider's business continuity and recovery plans, a regulated entity may not be able to recover or shift its operations in the face of a large-scale disruption.

The disruption of outsourced services could lead to losses if, for example clients are unable to access their accounts or have their orders executed during a period of market volatility.

(e) Returning to the office and a hybrid working environment

Several of the changes that occurred or were accelerated in response to the pandemic will continue to challenge operational resilience for regulated entities. A key change is the move to a steady-state work environment that may include a hybrid model of remote and office working. This model may provide benefits to both employees and regulated entities and the flexibility it provides may foster greater diversity and inclusion in the workforce of regulated entities and may result in cost savings for regulated entities in the form of reduced occupancy expenses. However, a hybrid, decentralized work environment raises similar challenges to remote working as described above[44][45][46].

As large scale remote and hybrid working are new for many regulated entities, the risks and controls are still being evaluated and tested. In this context, scenario analysis will continue to be an important tool in identifying risks and assessing the effectiveness of controls.

Risks to operational resilience

Regulated entities may not have fully considered the risk implications of having certain business functions performed remotely on a large scale and on a continuous basis. For instance, remote working may be less suitable for certain business functions, such as, where there is heightened risk of information leakage that is difficult to mitigate with individuals working from home. In addition, some regulated entities have reported difficulties with training and oversight of staff in a remote working environment.

As hybrid working models become normal practice in many jurisdictions the risks to operational resilience related to remote working will remain into the future.

---

43 Ibid 16 p5-6

44 Ibid 39

45 FMSB Hybrid working in FICC markets Future risk management frameworks September 2021, available at https://fmsb.com/wp-content/uploads/2021/09/Spotlight-Review-%E2%80%98Hybrid-working-in-FICC-markets-%E2%80%93-Future-risk-management-frameworks-.pdf

46 Hong Kong Securities and Futures Commission, *Report on Operational Resilience and Remote Working Arrangements*, October 2021, https://www.sfc.hk/-/media/EN/files/COM/Reports-and-surveys/Report_Operational-resilience-and-remote-working-arrangements_Oct-2021_EN.pdf. United Kingdom Financial Conduct Authority, *Remote or hybrid working: FCA expectations for firms*, 11/10/2021, https://www.fca.org.uk/firms/remote-hybrid-working-expectations .

Chapter 5 - Lessons Learned

When looking at the performance of regulated entities during the pandemic, IOSCO is of the view that they were largely successful in continuing their operations, despite the many significant disruptions and the unexpected nature and length of those disruptions.

IOSCO is of the view that the recommendations and sound practices in the Committee 2 Report and the standards, guidance and sound practices in the Committee 3 Report continue to be useful and relevant and the regulatory framework has worked well. However, the issues that were encountered during the pandemic reinforce the importance of planning for effective operational resilience.

As we move into the next phase of the pandemic (and beyond), new events may further inform the operational resilience considerations that regulated entities face. The pandemic has demonstrated that operations may not be fully restored for a prolonged period of time following a disruption, a disruption may impact all or multiple locations at the same time and that there may be fundamental changes as to how operations resume following a disruption.

IOSCO proposes the following lessons for regulated entities to take into consideration and to supplement the Committee 2 Report and the Committee 3 Report.

(a) Operational resilience means more than just technological solutions

Previous IOSCO work noted that in the context of operational resilience, trading venues "should consider [c]onducting assessments of the potential impact of material operational disruptions, particularly to critical systems, and taking account of these in developing the BCP" and that market intermediaries "[i]dentify the business functions and systems that are critical to continue operations in the face of a major operational disruption, along with primary and backup staff."

IOSCO believes that the experience of the pandemic has demonstrated that operational resilience depends not only on the resilience of technology, but also may depend on resilience of processes and personnel. The inability to follow established processes, or the loss of key personnel or a significant number of personnel, can disrupt operations. Planning how to manage these circumstances is as important as managing disruptions to technology or systems. This focus is consistent with the operational resilience work that has been published by financial regulators and other standard setters.

Considering the experiences during the pandemic, IOSCO believes that it is important for regulated entities to re-evaluate the operational resilience strategies and business continuity planning to incorporate any lessons learned. While business continuity planning is focused on recovery from a disruption, operational resilience also necessitates considering preventative measures with respect to disruptions.

(b) Consider dependencies and interconnectivity

Previous IOSCO work noted the importance of market intermediaries "[i]dentify[ing] the business functions and systems that are critical to continue operations in the face of a [disruption], along with primary and backup staff."[47]

When evaluating their approaches to operational resilience, it is important for regulated entities to consider their full business process and all dependencies throughout the supply chain (both internal and external) to adequately address risks and controls. As part of this process, it is important for entities to understand and map critical functions, internal and external dependencies, identify concentration risks and identify likely points of failures and options for reducing the risk.

In light of the differing operational experiences stemming from the pandemic, it is critically important for regulated entities to understand where key dependencies are located and where they reside with outsourced providers including understanding the recovery plans that outsourced providers have in place. It is important to have contingency plans in place for those times when off-shore third-party services or agreed third-party service levels may not be provided for a prolonged period of time, including scenarios where alternatives may be limited. This may include contemplating mechanics of onshoring where these functions cannot be provided and quickly providing training to new and redeployed staff.

We note that the pandemic has demonstrated that challenges to operational resilience for all regulated entities may be symmetrical as well as asymmetrical. For instance, a future challenge may be a scenario where all service providers suffer an outage and simply moving to a different service provider or backup location may not be an option to help ensure the delivery of critical operations through a disruption. Likewise, limitations or restrictions on the ability of regulated entities to carry on services may be more widespread than anticipated or planned for by regulated entities.

Under previous IOSCO work on trading venues' BCP, "[c]onsideration of the possibility that the services of a supplying firm (i.e., a firm to which critical systems have been outsourced) may become unavailable and setting forth in the SLA [service level agreement] the obligations of the supplying firm, should its services become unavailable, and if possible, providing for access to information by the Trading Venue of the supplying firm's own BCP, if any" were offered as a sound practice.

In addition, for market intermediaries, IOSCO stated that they should consider "[a]ssess[ing], on a periodic basis, the current robustness of their BCP, including critical outsourcing suppliers, to ensure high availability and resiliency of critical systems in times of an MOD …". It is important for regulated entities to re-evaluate, on an on-going and regular basis, their provisions related to the use of outsourced providers given their experiences during the pandemic. In addition, it is important for regulated entities to understand and regularly assess the robustness of supplying firms' operational resilience throughout the supply chain, identify geographic and vendor concentration risks, and minimize the impacts of the failure by one of these third parties.

---

47 See Committee 3 Report. Ibid. 13

(c) Review, update and test BCP

Once critical business functions, interdependencies, potential risks and options to manage them have been identified, regulated entities should review and update their BCP, as appropriate. Consistent with previous IOSCO work, it is important to regularly update BCP in light of changes to a regulated entity's operations, structure, business or operational environment. In the context of the pandemic, to date, a changing environment has included border closures, business lockdowns, extended work-from-home arrangements, spikes in trading volumes and extreme impacts on supply chains. In addition, it seems important to consider that pre-pandemic operations may not be restored for a prolonged period and the disruption may continue to impact all or multiple locations at a time.

Previous IOSCO work noted the importance of reviewing and testing BCP. Regulated entities may consider evaluating their processes to help ensure that they include a broad range of scenarios in order to facilitate operational resilience in light of the experiences during the pandemic, such as the restrictions, unavailability of back-up sites and the move to work from home. The pandemic revealed the importance of including some more extreme events in BCP scenario testing. Lessons learned from business continuity planning and resilience testing are important to update operational resilience frameworks. One such lesson was the importance of communication channels between regulators, key authorities, regulated entities and third-party service providers to help understand any impacts on operational resilience. For instance, this communication allowed for certain staff critical to operations to be designated as key workers and exempt from stay-at-home orders. Supervisors' evaluations of third-party service providers could assess both the service provider's plans for survival, as well as how regulated entities could operate in the absence of the third-party service provider or in the event that the third-party service provider suffers a significant disruption in its operations.

In addition, as part of their business continuity planning, updating and testing, it is important for regulated entities to obtain information regarding the BCP of their third-party service providers. As discussed above, reliance on these service providers necessitates understanding what their plans are should a disruption impact their operations or their ability to perform their obligations under service level agreements. Testing of BCP includes consideration of these third parties to facilitate the continuation of operations.

(d) Effective governance frameworks

As seen during the pandemic, there may be circumstances where quick and decisive decisions need to be made with limited information and without a clear view of what the future will bring. In these circumstances, it is important that regulated entities have an effective governance framework that allows decisions to be taken swiftly, at the appropriate level and in circumstances where decision makers are dispersed. It is important that an effective governance framework be supported with timely and reliable data and detailed insights into the full operations of the business to the extent possible.

It is important that where decisions are made quickly and risks are accepted with limited due diligence, that they are re-visited and appropriately back tested to help ensure they continue to be fit for purpose and consistent with the regulated entity's risk appetite.

(e) Compliance and supervisory processes

One of the challenges identified from the pandemic has been the continued dependence on manual processes and physical documents in certain circumstances. It is important for regulated entities to consider whether they can move such processes to an electronic form taking into account relevant laws. The review of processes is important to help ensure, among other things, that checks, and balances are in place to minimize the risks as systems change. Regulatory considerations may be implicated.

In addition, as part of planning for operational resilience in a pandemic scenario, it may be important for regulated entities to take into account supervision of decentralized and remote work, as well as a hybrid model where staff split their work time between the office and working remotely. For example, new policies may be appropriate, or existing policies may be adapted, to help ensure handling of confidential information, cyber security and communication among employees, stakeholders, clients, and regulators. It may be important to review whether current training regimes are adequate or may appropriate to be adapted.

Identifying key staff who are required to be on site during any future shutdown and working with regulators and other relevant authorities to ensure these individuals get appropriate designation may also be important to ensure that regulated entities can continue to perform their activities.

Finally, in some cases, new systems were deployed quickly, and solutions may have been adopted with little testing or limited due diligence. It may be important for regulated entities to back-test so as to confirm that the adopted systems are appropriate going forward and seek to ensure that any increased risk accepted during stressed conditions do not become inappropriately embedded in the entity's operations without full testing.

(f) Information security risk

Challenges in relation to information security were also exposed during the pandemic. The shift to remote working often required the implementation of new technology as well as the use of personal equipment. This has increased the risk of unauthorized persons gaining access to information about clients, transactions, or trading.

As with the compliance and supervisory processes, new policies may be appropriate, or existing policies may be adapted, to help ensure handling of confidential information, cyber security and communication among employees, stakeholders, clients, and regulators.

Chapter 6 - Conclusion

Operational resilience is essential to the functioning to the financial system and supports financial stability, market integrity and investor protection. The impact of COVID-19 was global and affected every sector of the financial system and wider economy. This event increased firms and regulators' attention to operational resilience and also presented an opportunity to identify lessons about how improve operational resilience going forward.

This report has summarised the existing operational resilience work by IOSCO and other international organizations, to help identify the extent to which a consistent, and hence more efficient, approach to operational resilience can be taken. It outlines how the pandemic impacted regulated entities and the key operational risks and challenges that regulated entities faced during the pandemic. Building on this and the IOSCO and other international organizations' operational resilience principles and guidance, the report has set out some observations and lessons learned from the pandemic that should inform regulated entities' operational resilience arrangements going forward.

While the COVID-19 pandemic increased the focus on operational resilience, there is a range of other disruptions or unforeseen events that can impact on operational resilience such as natural disasters and geo-political events. Operational resilience is an IOSCO board priority and IOSCO will continue to monitor developments and develop work as necessary.

APPENDIX A

Global Regulatory Initiatives on Operational Resilience

- **Joint Forum BCP Principles**
- **U.S. Interagency paper on Sound Practices to Strengthen Operational Resilience**
- **C2 Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity**
- **C3 Market Intermediary Business Continuity and Recovery Planning**
- **FSB Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective**

	Governance
BCBS Principles for Operational Resilience (March 2021)	Principle 1: Banks should utilize 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 minimize their impact on delivering critical operations through disruption.
BCBS Revisions to the Principles for the Sound Management of Operational Risk	Principle 1: The board of directors should take the lead in establishing a strong risk management culture, implemented by senior management. The board of directors and senior management should establish a corporate culture guided by strong risk management, set standards and incentives for professional and responsible behavior, and ensure that staff receives appropriate risk management and ethics training Principle 3: The board of directors should approve and periodically review the operational risk management framework, and ensure that senior management implements the policies, processes and systems of the operational risk management framework effectively at all decision levels. Principle 5: Senior management should develop for approval by the board of directors a clear, effective and robust governance structure with well-defined, transparent and consistent lines of responsibility. Senior management is responsible for consistently implementing and maintaining throughout the organization policies, processes and systems for managing operational risk in the bank's material products, activities, processes and systems consistent with the bank's risk appetite and tolerance statement
U.S. Interagency Paper on Sound Practices to Strengthen Operational Resilience (November 2020)	Effective governance helps ensure that firms not only operate in a safe and sound manner and comply with applicable laws and regulations, but also maintain operational resilience

C2 Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (December 2015)	Effective governance is essential both in the context of management of critical systems and the establishment of BCP. Many Trading Venues have a dedicated officer (e.g., Chief Risk Officer (CRO) or Chief Operating Officer (COO)), separate from those responsible for IT matters, who is responsible for the development and ongoing review (updating) of the BCP. Alternatively, Trading Venues may have risk management committees responsible for the approval of a BCP and related procedures. Trading Venues should consider establishing an appropriate governance structure for the approval of the BCP and any updates
C3 Market Intermediary Business Continuity and Recovery Planning (December 2015)	Sound practices for BCP that merit consideration include: 1) establishing an appropriate internal corporate governance structure that will be capable of implementing the BCP successfully in the event of a MOD. This could include having the firm designate certain individuals who are responsible for business continuity management. 2) Establish policies and procedures to ensure that critical personnel (or their back-ups) are available in the event of a MOD.
Joint Forum BCP Principles (August 2006)	Principle 1: Financial industry participants and financial authorities should have effective and comprehensive approaches to business continuity management. An organization's board of directors and senior management are collectively responsible for the organization's business continuity
FCA Building Operational Resilience: Impact Tolerances for Important Business Services (December 2019)	Firms' boards and senior management should be sufficiently engaged in setting effective standards for operational resilience. The board and senior management should have sufficient time to establish the business and risk strategies and the management of the main risks relevant to operational resilience. Firms should ensure that in meeting their responsibilities, board members and senior management have the knowledge, experience and skills necessary for the discharge of the responsibilities allocated to them.
	Operational Risk Management
BCBS Principles for Operational Resilience (March 2021)	Principle 2**:** 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 expectations.
BCBS Revisions to the Principles for the Sound Management of Operational Risk	Although operational risk management and operational resilience address different goals, they are closely interconnected. An effective operational risk management system and a robust level of operational resilience work together to reduce the frequency and the impact of operational risk events.

	Principle 2: Banks should develop, implement and maintain an operational risk management framework that is fully integrated into the bank's overall risk management processes. The ORMF adopted by an individual bank will depend on a range of factors, including the bank's nature, size, complexity and risk profile Principle 4: The board of directors should approve and periodically review a risk appetite and tolerance statement for operational risk that articulates the nature, types and levels of operational risk the bank is willing to assume Principle 6: Senior management should ensure the comprehensive identification and assessment of the operational risk inherent in all material products, activities, processes and systems to make sure the inherent risks and incentives are well understood. Principle 9: Banks should have a strong control environment that utilizes policies, processes and systems; appropriate internal controls; and appropriate risk mitigation and/or transfer strategies
U.S. Interagency Paper on Sound Practices to Strengthen Operational Resilience (November 2020)	By identifying, managing, and mitigating operational risk exposures related to internal processes, people, systems, external threats, and third parties, a firm is able to strengthen its operational resilience. Effective operational risk management involves close engagement by the firm's senior management, business line operations, independent operational risk management function, and independent internal (or external) audit function.
C2 Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business Continuity (December 2015)	Trading venues should consider establishing objectives and strategies in terms of business continuity planning, which should include allocation of adequate human, technological and financial resources to the development, maintenance, updating and testing of the BCP
C3 Market Intermediary Business Continuity and Recovery Planning (December 2015)	Sound practices for BCP that merit consideration include: 1) Identifying the business functions and systems that are critical to continue operations in the face of a MOD, along with primary and backup staff 2) Identifying the major threats and impacts posed to the firm 3) Assess the potential impact of a MOD through qualitative and quantitative analysis
Joint Forum BCP Principles (August 2006)	Principle 2: Financial industry participants and financial authorities should incorporate the risk of a major operational disruption into their approaches to business continuity management. Financial authorities' business continuity management also should address how they will respond to a major operational disruption that affects the operation of the financial industry participants or financial system for which they are responsible.

FCA Policy Statement (PS21/3) on Building Operational Resilience (March 2021)	Firms should identify their important business services that if disrupted could cause harm to consumers or risk to market integrity Firms should set impacts tolerances for providing important business services in order to consider what a firm would do when a disruptive event occurs. Impact tolerance describes the maximum tolerable level of disruption to an important business service, assuming disruption to the supporting systems and processes will occur. Firms should set their impact tolerances at the first point at which a disruption to an important business service would cause intolerable levels of harm to consumers or risk to market integrity. Firms should use impact tolerances as a planning tool and should assure themselves they are able to remain within them in severe but plausible scenarios.
FSB Lessons Learnt from the COVID-19 Pandemic from a Financial Stability Perspective	COVID-19 has reinforced the importance of continuing to promote resilience amidst rapid technological change in the economy and the global financial system. Work-from-home arrangements and demand for online banking services propelled the adoption of new technologies and accelerated digitalization in financial services. While outsourcing to third-party providers, such as cloud services, seems to have enhanced operational resilience at financial institutions, increased reliance on such services may give rise to new challenges and vulnerabilities. Effective management of such risks across the supply chain is essential for maintaining operational resilience and addressing cyber and information and communication technology (ICT) related vulnerabilities.
	Business Continuity Planning
BCBS Principles for Operational Resilience (March 2021)	Principle 3**:** 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.
BCBS Revisions to the Principles for the Sound Management of Operational Risk	Principle 11: Banks should have business continuity plans in place to ensure their ability to operate on an ongoing basis and limit losses in the event of a severe business disruption. Business continuity plans should be linked to the bank's operational risk management framework.
U.S. Interagency paper on Sound Practices to Strengthen Operational Resilience (November 2020)	Business continuity plans consider market- and enterprise-wide stresses and idiosyncratic risks that can imperil the continuity of a firm's critical operations and core business lines or otherwise have a broader impact on the financial system. A firm that is subject to recovery or resolution planning requirements can leverage the information in these plans for business continuity management purposes.
C2 Mechanisms for Trading Venues to Effectively Manage Electronic Trading Risks and Plans for Business	Trading venues should consider testing the operation of the BCP on a periodic basis. BCP testing could include assessments of the Trading Venue's ability to recover from incidents under predefined objectives and the ability of a Trading Venue to resume trading within the target recovery time. In addition: a) documenting and recording the testing results and submitting them promptly to the Board of Directors or other competent management body

Continuity (December 2015)	b) making the results available to the regulator upon request c) coordinating, as appropriate for its market structure, the testing of its BCP with participants and with other venues
C3 Market Intermediary Business Continuity and Recovery Planning (December 2015)	Sound practices for BCP that merit consideration include: Assess, on a periodic basis, the current robustness of their BCP, including critical outsourcing suppliers, to ensure high availability and resilience of critical systems in times of a MOD, including the testing of the market intermediary's BCP on a periodic basis. Whenever practical and useful, participate in industry-wide or cross-border testing with other intermediaries and stakeholders, and conduct mock drills (simulation exercises) to test the effectiveness of the BCP plan. Senior management should review results of BCP assessments. Considering the unique aspects of regional operations if it is a globally active firm. For example, consider the need to have separate BCP for different markets in which the firm operates.
Joint Forum BCP Principles (August 2006)	Principle 6: Financial industry participants and financial authorities should test their business continuity plans, evaluate their effectiveness, and update their business continuity management, as appropriate.
Committee on Payments and Market Infrastructures Board of the International Organization of Securities Commissions Implementation monitoring of PFMI: Level 3 assessment of FMIs' business continuity planning	The report finds that all the surveyed FMIs have operational reliability objectives, focusing on system availability and recovery time. FMIs reportedly review their business continuity plans at least annually and test them regularly. However, the report found that some FMIs do not fully meet expectations with respect to recovery from operational incidents, such as natural disasters or IT systems outage. In particular, the business continuity management of some, and potentially many, FMIs do not seem to aim to resume operations in a timely way, including in the event of a wide-scale or major disruption. This is a serious area of concern and the CPMI and IOSCO expect the relevant FMIs and their supervisors to address this as a matter of the highest priority.

APPENDIX B

Feedback Statement

IOSCO received 12 written responses to the Consultation Report and had a number of engagements with other international bodies and industry associations. Most respondents agreed with the observations identified in the Report and were supportive of the proposed IOSCO lessons learned. Some respondents suggested minor changes as well as raising additional impacts, risks and challenges they observed during the pandemic. IOSCO amended the report in response to the feedback. Below is a summary of the key feedback received for each question.

Q1: In the context of reviewing operational resilience during the pandemic, is the description of 'operational resilience' and 'critical operations' appropriate for:

(a) trading venues;

(b) market intermediaries?

If not, please explain why and describe your preferred approach?

IOSCO received near universal agreement that the descriptions of operational resilience and critical operations are appropriate. Some respondents suggested the definitions could be expanded further to be more prescriptive as well as further align with the BCBS. It was also suggested that related concepts should also be defined. One respondent also suggested that we discuss business continuity management (BCM) and not just BCP. We considered that this is addressed in the Committee 2 and Committee 3 Reports referenced in this Report.

One respondent noted some regulators' definitions have departed from the BCBS. Another respondent agreed that the definitions were helpful but cautioned that any further policy work would not be helpful or desirable, instead regulated entities should make their own determinations.

Q2: Are there other impacts, risks or challenges faced by regulated entities not mentioned in this section?

There was no disagreement with the impacts, risks and challenges IOSCO identified. Respondents raised various other impacts, risks and challenges. In particular, some drew out additional aspects of third-party and cyber related risks related to remote working.

Q3: Are there other impacts, risks or challenges from remote work or hybrid working that impact operational resilience?

Respondents identified a wide range of other impacts, risks and challenges – there was some overlap with responses to question two. One additional challenge identified by several respondents was the ongoing reliance on paper-based processes and face-to-face interactions particularly where regulatory relief is wound back or withdrawn. Respondents also identified the reliance of remote working infrastructure including hardware, internet service providers, and electricity providers as a key challenge. Maintaining corporate culture, training new staff and staff well-being were also identified as challenges. One respondent highlighted the increased talent pool available that remote working provides. These observations have been addressed in the Report.

Q4: Are there other lessons learned that can be drawn from the experiences of regulated entities during the pandemic in the context of maintaining operational resilience?

Responses identified that BCP was critical to managing the disruption caused by the pandemic. The experience has resulted in BCP becoming stronger during the pandemic. One response highlighted the broader importance of business continuity management, of which BCP is one aspect. Respondents expressed that regulatory relief and guidance was important and implementing this on a permanent basis should be considered. Some respondents identified that the regulatory approach should remain flexible and restrictions can have unforeseen and undesirable consequences. Collaboration and communication between regulated entities, regulators, third-party providers and other government agencies was also very important.

In addition to providing responses to the specific questions in the Consultation Report, some respondents made broader observations about operational resilience and cyber security. IOSCO considered the feedback in settling the Report.