April 1, 2024

Submitted via CFTC Comments Portal

Christopher Kirkpatrick
Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street, N.W., Washington, D.C. 20581

**Re: Operational Resilience Framework for Futures Commission Merchants, Swap Dealers and Major Swap Participants**

Dear Mr. Kirkpatrick,

The Global Financial Markets Association ("GFMA")[1] supports the Commodity Futures Trading Commission's (the "Commission") stated aim to provide a principles-based approach in its rule proposal for requirements for an Operational Resilience Framework ("ORF") for Futures Commission Merchants ("FCMs"), Swap Dealers ("SDs"), and Major Swap Participants ("MSPs") (the "Proposal").[2] GFMA believes that the Commission's aim for a principles-based approach is consistent with other international regulatory efforts on operational resilience,[3] which GFMA fully supports. GFMA welcomes the opportunity to comment on the Proposal and offer recommendations to align the Proposal with the Commission's stated goal to develop a principles-based rule. GFMA is also aware that the Securities Industry and Financial Markets Association ("SIFMA") and the Institute of International Bankers ("IIB") are

---

1 The GFMA represents the common interests of the world's leading financial and capital market participants, to provide a collective voice on matters that support global capital markets. We advocate on policies to address risks that have no borders, regional market developments that impact global capital markets, and policies that promote efficient cross-border capital flows, benefiting broader global economic growth. The Global Financial Markets Association ("GFMA") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London, Brussels and Frankfurt, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and Singapore, and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA.

2 Operational Resilience Framework for Futures Commission Merchants, Swap Dealers, and Major Swap Participants, 89 Fed. Reg. 4706 (Jan. 24, 2024) [hereinafter *Proposing Release*].

3 *See, e.g.*, Basel Committee on Banking Supervision, Principles for Operational Resilience, at 3 (March 2021), https://www.bis.org/bcbs/publ/d516.pdf [hereinafter *Principles for Operational Resilience*]; SR 20-24, *Sound Practices to Strengthen Operational Resilience* (Nov. 2, 2020), available at https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm.

submitting a comment on the Proposal (the "SIFMA and IIB Letter"). GFMA fully aligns with and supports the recommendations in the SIFMA and IIB Letter.

GFMA appreciates the importance of operational resilience for the public and private sectors to maintain confidence in the financial industry and to support financial stability and economic growth. We and our members are fully committed to ensuring robust operational resilience and already deploy a wide variety of policies, procedures, systems and controls to ensure "the ability to deliver critical operations through disruption."[4] Indeed, we are consistently and closely engaged with global standard-setters and regulators on operational resilience. As such, we are keenly aware of the depth and breadth of the work international regulators are currently doing in the operational resilience space and believe harmonization is in the interest of both regulators and firms. These pre-existing frameworks are the product of not only recognition among our members that operational resilience is good for business, but also that many entities regulated by the Commission are already, or will shortly be, subject to operational resilience requirements that would overlap with those proposed by the Commission. To that end, we have included an Appendix to this letter that highlights relevant regulations and guidance that financial firms already comply with globally and that reflect the resilience capabilities that firms have developed over time.

To ensure that the Commission's Proposal achieves its stated aim to establish principles-based operational risk management provisions that protect derivatives markets and the institutions and customers therein, it is essential that the Commission aligns with the wider regulatory landscape. For example, it is critical that covered entities are able to communicate internally, and with their regulators, about operational resilience matters on a common linguistic and principled basis. At present, however, GFMA is concerned that the Proposal may destabilize established and developing international standards in operational resilience, as the Proposal risks creating both unnecessary regulatory overlap[5] as well as divergence in terminology and substance from existing regimes. This dislocation, rather than improving operational resilience outcomes, risks increasing the compliance burden on covered entities in order to deal with disparate regimes and will instead impede operational resilience due to focusing on navigating conflicting standards instead of on the substance of resilience.

GFMA's concern with alignment is particularly acute relative to the Proposal's definitions. To begin, GFMA agrees with SIFMA and IIB that the Proposal would

---

4 Principles for Operational Resilience, *supra* note 2, at 3.

5 For example, covered entities under the Proposal are already subject to NFA requirements on information security, third-party risk management, and business continuity and disaster recovery. *See* National Futures Association, *Interpretive Notice to NFA Compliance Rules 2-9, 2-36 and 2-49*, available at https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

benefit from a clear definition of operational resilience that reflects the existing definition in the Basel Committee on Banking Supervision's *Principles for Operational Resilience*: "the ability of a [covered entity] to deliver critical operations through disruption." GFMA believes the Basel Committee's definition appropriately limits the scope of its definition of operational resilience to "critical operations" and "critical functions," in turn helping to define the people, processes and communication channels necessary to support effective engagement.

Next, the Proposal's existing definitions are both overly broad and misaligned with international definitions. Specifically, GFMA is concerned with the scope of the definitions for "incident," "covered technology," "covered information," the incident "notification trigger" and "critical third-party service provider." GFMA believes that the current definitions for these terms are likely to result in undue compliance burdens, as the use of defined terms will flow through various regulatory provisions, creating asymmetry with the other regulations and guidance that firms are complying with in parallel. Therefore, GFMA strongly encourages the Commission to revise the definitions in accordance with existing, widely used terminology, as put forward by the SIFMA and IIB Letter.

Moreover, the need for broad regulatory convergence is also reflected in the significant efforts undertaken by the Financial Stability Board through its Format for Incident Reporting Exchange ("FIRE") initiative, which aims to reduce regulatory fragmentation and achieve global standardization of cyber incident reporting requirements between regulatory authorities and financial institutions, a process being spearheaded by, among others, Andrew Bailey, Chair of the Financial Stability Board Standing Committee on Supervisory and Regulatory Cooperation.

Finally, GFMA is concerned that the Proposal's six-month implementation period is too short to allow covered entities to successfully obtain substituted compliance determinations and, instead, will leave entities that have submitted applications in good faith waiting for confirmation for some period of time after the implementation period has ended. For example, recent experience with capital and financial reporting requirements has shown that the timeline for substituted compliance tends to be years, not months. As such, the Proposal fails to fully reflect the wide range of obligations that covered entities are already subject to, and while GFMA's members are confident that substituted compliance would be granted, they are concerned about the time it would take were the rule to come into effect as proposed. GFMA therefore supports the SIFMA and IIB Letter's request for an extended and phased implementation timeframe.

*******

As noted at the outset, GFMA welcomes the opportunity to comment on the Proposal. We appreciate the Commission's consideration of our comments from a global regulatory perspective and hope that they serve as an aid to the Commission's deliberations. GFMA would welcome the opportunity to continue to participate in this valuable process. Please feel free to contact the undersigned to discuss these issues further.

Sincerely,

Allison Parent
Executive Director
GFMA

cc: The Honorable Rostin Behnam, Chairman
The Honorable Kristin N. Johnson, Commissioner
The Honorable Christy Goldsmith Romero, Commissioner
The Honorable Summer K. Mersinger, Commissioner
The Honorable Caroline D. Pham, Commissioner
Ms. Amanda Olear, Director, Market Participants Division
Ms. Pamela Geraghty, Deputy Director

## Appendix

This Appendix does not include the Commission's Proposal, which is the subject of the main letter, but includes other relevant documents for context. For the avoidance of doubt, this Appendix, as illustrative as it is across jurisdictions on the regulatory governance processes that members manage to today, is not intended as an exhaustive listing of all relevant documents.

| Financial Regulations and Resilience Capabilities by theme/functional area | | |
|---|---|---|
| **Functional Area** | **Regulation/Guidance** | **Resilience Capabilities** |
| Operational resilience | NFA Interpretive Notice 9070 and NFA Compliance Rules 2-9, 2-36 and 2-49 | • Establish and implement a governance framework that supports informed decision-making and escalation to identify and manage information security risks.<br>• Adopt and enforce a written information system security plan. |
| | Bank of England, Prudential Regulation Authority (PRA) – Operational resilience: Impact tolerances for important business services | • Consider the stability of the UK financial system when setting impact tolerances.<br>• Review important business services annually at a minimum. |
| | Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, Office of the Comptroller of the Currency – Sound Practices to Strengthen Operational Resilience (October 2020) | • The paper outlines practices to increase operational resilience that are drawn from existing regulations, guidance, statements, and common industry standards.<br>• The practices are grounded in effective governance and risk management techniques, consider third-party risks, and include resilient information systems. The paper does not revise the agencies' existing rules or guidance.<br>• The practices are for domestic banks with more than $250 billion in total consolidated assets or banks with more than $100 billion in total assets and other risk characteristics. |
| | Basel Committee on Banking Supervision (BCBS) – Principles for Operational Resilience (August 2020) | • Seek to promote a principles-based approach to improving operational resilience.<br>• Build on the Committee's Principles for the Sound Management of Operational Risk (PSMOR), principles on corporate governance for banks, outsourcing, business continuity and relevant risk management-related guidance. |
| | Monetary Authority of Singapore (MAS) - Ensuring Safe Management and Operational Resilience of the Financial Sector (2020) | • Issue guidance and advisories to address operational, technology and cyber risks.<br>• Focus our surveillance, supervision and enforcement efforts on financial institutions' pandemic response as well as operational and cyber resilience.<br>• Continue to monitor the impact of COVID-19 and put in place additional measures and advisories as necessary. |

| | | |
|---|---|---|
| | European Commission – Digital Operational resilience framework for financial services (November 2022) | • Implement a comprehensive ICT risk management framework, which is integrated into the overall risk management system.<br>• Establish and implement a management process to monitor, manage and notify ICT-related incidents.<br>• Develop a harmonized digital operational resilience testing framework.<br>• Enhance oversight of critical third-party providers. |
| Risk Governance | Basel Committee on Banking Supervision (BCBS) – Corporate Governance Principles for banks (July 2015) | • Ensure sound and robust corporate governance by determining allocation of authority and responsibilities, including: i/ setting the banks strategy and objectives; ii/ selecting and overseeing personnel; iii/ operating the bank on a day-to-day; iv/ protecting recognized stakeholders; v/ aligning corporate culture; vi/ establishing control functions.<br>• Reinforce the collective oversight and risk governance responsibilities of the board (e.g., risk governance, risk culture, risk appetite, risk capacity).<br>• Evaluating and promoting a strong risk culture in organizations. |
| | Financial Conduct Authority (FCA) - The Senior Managers and Certification Regime (July 2019) | • Provide a robust framework for accountability and transparency<br>• Ensure accountability from the most senior individual responsible for managing the internal operations and technology of a firm. |
| | Federal Reserve Board (FRB) – "Three Lines of Defense" Risk Management Model | • Ensure systemically important financial institutions (SIFIs) manage risk in a way that is prudent and consistent with their business strategy and risk tolerance.<br>• Clarify the responsibility of the executive management team in managing the overall risk framework. |
| | The Office of the Comptroller of the Currency (OCC) - Heightened Standards for Large Financial Institutions (September 2014) | • Guidelines to strengthen the governance and risk management practices of large financial institutions.<br>• The guidelines provide that covered institutions should establish and adhere to a written risk governance framework to manage and control its risk-taking activities.<br>• The guidelines also provide minimum standards for the institutions' boards of directors to oversee the risk governance framework. |
| | IAIS – Application Paper on Proactive Supervision of Corporate Governance (February 2019) | • Calls upon insurance supervisors to be forward-looking, identify issues early and act quickly and constructively to address circumstances before they become critical or a violation of law or local requirements. |

| | | |
|---|---|---|
| Risk Monitoring and Management | FSB – Principles for an effective risk appetite framework (November 2013) | • The FSB Principles set out key elements for: (i) an effective risk appetite framework; (ii) an effective risk appetite statement; (iii) risk limits; and (iv) defining the roles and responsibilities of the board of directors and senior management.<br>• The Principles aim to enhance the supervision of systemically important financial institutions but are also relevant for the supervision of financial institutions and groups more generally, including insurers, securities firms and other non-bank financial institutions. |
| | Basel Committee on Banking Supervision (BCBS) - Principles for the Sound Management of Operational Risk (June 2011) | • Ensure that financial institutions identify risks to the bank and measure exposures to those risks (where possible) and ensure that an effective capital planning and monitoring program is in place to monitor risk exposures and corresponding capital needs on an ongoing basis, take steps to control or mitigate risk exposures and report to senior management and the board on the bank's risk exposures and capital positions. |
| | Basel Committee on Banking Supervision (BCBS) - Revisions to the principles for the sound management of operational risk (March 2021) | • Identifies principles that have not been adequately implemented, and provides further guidance to facilitate implementation (e.g., risk identification and assessment tools, change management programs and processes, implementation of the three lines of defense, senior management oversight, articulation of operational risk appetite and tolerance statements, risk disclosure).<br>• Captures additional important sources of operational risk, such as those arising from information and communication technology (ICT) risk, warranting the introduction of a specific principle on ICT risk management. |
| Business Continuity Planning, Systems Integrity and Third-Party Resilience | Federal Reserve Board, Office of the Comptroller of the Currency, Securities and Exchange Commission – Interagency Guidance on Third-Party Relationships: Risk Management (June 2023) | • Engage in comprehensive and rigorous oversight and management of third-party relationships that support higher-risk activities, including critical activities.<br>• Incorporate independent reviews, documentation and reporting, and oversight and accountability into third-party risk management planning. |
| | Financial Stability Board – Enhancing Third-Party Risk Management and Oversight: A toolkit for financial institutions and financial authorities (December 2023) | • Identify critical services consistently yet flexibly.<br>• Consistent mapping of financial institutions' third-party service relationships.<br>• Conduct due diligence, contracting and ongoing monitoring of critical services and service providers.<br>• Manage risks relating to third-party service providers' use of service supply chains.<br>• Implement and test business continuity plans and coordinate with third-party service providers for their business continuity. |

| | | |
|---|---|---|
| | The Joint Forum (BCBS, IOSCO, IAIS) – High-Level Principles for Business Continuity (August 2006) | • Ensure the development of recovery objectives that reflect the risk an event represents to the economy.<br>• Require the conducting of periodic tests of business continuity plans to ensure the plans are effective. |
| | The Joint Forum (BCBS, IOSCO, IAIS) – Outsourcing in Financial Services (February 2005) | • Reduce potential for over-reliance on outsourced activities that are critical to the ongoing viability of a regulated entity (e.g., draw up comprehensive and clear outsourcing policies, establish effective risk management programs, require contingency planning by the outsourcing firm, negotiate appropriate outsourcing contracts, and analyze the financial and infrastructure resources of the service provide).<br>• Mitigate concerns by ensuring that outsourcing is adequately considered in firm assessment whilst taking account of concentration risks in third-party providers when considering systemic risk issues. |
| | IOSCO – Principles on Outsourcing: Final Report (October 2021) | • Set out expectations for regulated entities that outsource tasks, along with guidance for implementation.<br>• Seven fundamental principles covering issues such as the definition of outsourcing, assessment of materiality and criticality, affiliates, sub-contracting, and outsourcing on a cross-border basis. |
| | Federal Financial Institutions Examination Council (FFIEC) – Business Continuity Guidelines | • Decrease the likelihood that disruptions will have a material and long-lasting impact on critical business services.<br>• Require institutions to assess all business functions, identify the impact of business disruptions and estimate maximum allowable downtime and recovery time objectives. |
| | Federal Financial Institutions Examination Council (FFIEC) - Information Technology Examination Handbook: Business Continuity Management | • Describe principles and practices for IT and operations for safety and soundness, consumer financial protection, and compliance with applicable laws and regulations.<br>• Focus on enterprise-wide, process-oriented approaches that consider technology, business operations, testing, and communication strategies critical to the continuity of the entire entity. |

| | | |
|---|---|---|
| | Federal Reserve System, U.S. Treasury Office of the Comptroller of the Currency, and the Securities and exchange Commission (SEC) – Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System (April 2003) | • Ensure rapid recovery and timely resumption of critical operations and staff following a wide-scale disruption for firms that play significant roles in critical financial markets.<br>• Require firms have a high level of confidence, through ongoing use or robust testing, that critical internal and external continuity arrangements are effective and compatible. |
| | Monetary Authority of Singapore (MAS) - Business Continuity Guidelines (June 2003) | • Ensure BCM is a risk-based framework that addresses operational risk by developing clear policies, strategies, and accountabilities for the recovery of critical business functions. |
| | Monetary Authority of Singapore (MAS) – Guidelines on Business Continuity Management (June 2022) | • Set expectations of how an FI's are to identify business functions that are critical and prioritize for recovery in disruption.<br>• Place greater emphasis on the Board of directors and senior management to demonstrate leadership and commitment in building an organizational culture that embeds business continuity.<br>• Expect FIs to have in place end-to-end business continuity plans for each service that is delivered to their customers.<br>• Continue to expect an FI to conduct different types of testing to gain the confidence that they will be able to continue to operate reliably, responsively, and efficiently as planned. |
| | Security Exchange Commission (SEC) – Regulation Systems Compliance and Integrity (Regulation SCI) (February 2015) | • Requires SCI entities (including registered clearing agencies) to establish written policies and procedures reasonably designed to ensure their systems have levels of capacity, integrity, resilience, availability and security adequate to maintain their operational capability.<br>• Require SCI entities to mandate participation by designated members or participants in scheduled testing of the operation of their BC/DR plans, including backup systems, and to coordinate such testing on an industry- or sector-wide basis with other SCI entities.<br>• Require SCI entities to develop business continuity and disaster recovery plans that include maintaining backup and recovery capabilities sufficiently resilient and geographically diverse to ensure next business day resumption of trading and two-hour resumption of clearance and settlement services following a wide-scale disruption. |

| | | |
|---|---|---|
| | European Banking Authority (EBA) – Outsourcing Guidelines (February 2015) | • Set standards for the management of outsourcing risk.<br>• Define requirements for competent authorities to effectively supervise financial institutions' outsourcing arrangements, including identifying and monitoring risk concentrations at individual service providers and assessing whether or not such concentrations could pose a risk to the stability of the financial system. |
| | European Securities Market Authority (ESMA) - Guidelines on Outsourcing to Cloud Service Providers (October 2021) | • Guidance on outsourcing to cloud service providers.<br>• Support firms identify, address and monitor the risks that may arise from their cloud outsourcing arrangements. |
| | Prudential Regulatory Authority (PRA) – Outsourcing and third party risk management (December 2019) | • Complement proposals on operational resilience<br>• Facilitate greater resilience and adoption of the cloud and other new technologies.<br>• Implement EBA "Outsourcing Guidelines" with consideration to, proportionality, governance/record keeping, outsourcing arrangements, data security, access/audit/information rights, sub-outsourcing, and business continuity/exit planning. |
| | EIOPA – Guidelines on Outsourcing Cloud Service Providers (February 2020) | • EIOPA Guidelines provide direction on cloud services and outsourcing, including the need for: a thorough pre-outsourcing analysis and risk assessment; a written outsourcing policy; notification to the supervisory authority of the outsourcing of critical or important operational functions and activities to Cloud Service Providers (CSPs); documentation requirements; due diligence and contractual considerations; exit strategies; access and audit rights; and data and system security. |
| Cyber Resilience and Risk Management | Federal Financial Institutions Examination Council – Information Security Handbook – Information Security Program Management | • Develop and implement a process to identify risk.<br>• Develop risk measurement processes that evaluate the inherent risk to the institution.<br>• Develop and implement appropriate controls to mitigate identified risks. |
| | New York Department of Financial Services (NYDFS) – Part 500 – Cybersecurity Requirements for Financial Services Companies (amended November 2023) | • Annual reporting to the board on plans for remediating material inadequacies.<br>• Board must exercise oversight of cybersecurity risk management.<br>• Maintain a cybersecurity program designed to protect the confidentiality, integrity and availability of the covered entity's information systems and nonpublic information<br>• Risk assessments reviewed and updated annually. |
| | Securities and Exchange Commission – Requirements to Address Cybersecurity Risks for Public Companies (adopted July 2023), | • Separate rules for public companies, registered investment advisers, broker-dealers, and swap participants.<br>• Rules generally cover cybersecurity risk management, strategy, governance, and incidents.<br>• Disclosures regarding risk management policies and procedures. |

| | | |
|---|---|---|
| | Registered Investment Advisers (proposed March 2022), and Market Participants (proposed March 2023). | • Disclosures regarding cybersecurity incidents. |
| | Office of the Comptroller of the Currency – Computer-Security Incident Notification Requirements (November 2021) | • Requires covered entities to disclose cybersecurity incidents within 72 hours. |
| | FSB – Cyber Lexicon (November 2018) | • Set of 50 core terms related to cyber security and cyber resilience.<br>• Support the work of the FSB, standard-setting bodies, authorities and private sector participants, to address financial sector cyber resilience. |
| | FSB – Effective Practices for Cyber Incident Response and Recovery (April 2020) | • Provide a toolkit of effective practices to assist financial institutions before, during and after a cyber incident.<br>• Set 46 effective practices, structured across: i/ Governance; ii/ Preparation; iii/ Analysis; iv/ Mitigation; v/ Restoration; vi/ Improvement; and vii/ Coordination and communication. |
| | G7 - Fundamental Elements of Cybersecurity for the Financial Sector (October 2016) | • Require firms to identify functions, activities, products and services — including interconnections, dependencies, and third parties — prioritize their relative importance and assess their respective cyber risks.<br>• Require firms to identify and implement controls — including systems, policies, procedures and training — to protect against and manage cyber risks within the tolerance set by the governing authority. |
| | G7 – Fundamental Elements for effective assessment of Cybersecurity in the Financial Sector (October 2017) | • Describe desirable outcomes for mature entities: i/ G7 fundamental elements are in place; ii/ cybersecurity influences organizational decision-making; iii/ understanding that disruption will occur, iv/ an adaptive cybersecurity approach is adopted; and v/ there is a culture that drives secure behaviors.<br>• Provide assessment components for assessors, to develop approach to assessing progress as entities build and enhance their cybersecurity: i/ establish clear assessment objectives; ii/ set and communicate methodology and expectations; iii/ maintain a diverse and process for toolkit selection; iv/ report clear findings and concrete remedial actions; and v/ ensure assessments are reliable and fair. |
| | G7 – Fundamental Elements for threat-led penetration testing (October 2018) | • Provide guidance for the assessment of resilience against malicious cyber incidents through simulation and testing (Threat-Led Penetration Testing).<br>• Enhance and assess cyber resilience of entities in the financial sector through guidance on: i) scoping and risk management; ii) resourcing; iii) threat intelligence; iv) penetration testing; v) close and remediation; and vi) thematic data. |

| | | |
|---|---|---|
| | Bank of England (BoE) CBEST (2016)<br>European Central Bank (ECB) TIBER-EU (May 2018) | • Provide standard approaches for regulatory-driven penetration testing regimes. |
| | European Central Bank (ECB) Cyber Resilience Oversight Expectations for Financial Market Infrastructures (CROE) (December 2018) | • Sets standards for the management of cybersecurity risks.<br>• Provide FMIs with detailed steps on how to operationalize the guidance, ensuring they are able to foster improvements and enhance their cyber resilience over a sustained period of time.<br>• Provide overseers with clear expectations to assess the FMIs for which they are responsible.<br>• Provide the basis for a meaningful discussion between the FMIs and their respective overseers. |
| | IAIS – Application Paper on Supervision of Insurer Cybersecurity (November 2018) | • Provide seven elements of insurer cybersecurity practices: a strategy and framework; governance; risk and control assessment; monitoring; response; recovery; information sharing and continuous learning.<br>• The Application Paper also includes supervisory case studies of effective practices. It notes that cyber resilience must be achieved by all insurers, regardless of size, specialty, domicile or geographic reach. Supervision of cyber resilience should be proportionate and risk-based. |
| Technology Risk Management | European Banking Authority (EBA) – Guidelines on ICT and security risk management (November 2019) | • Set minimum standards for the management of Information and Communication Technology (ICT) and security risk management.<br>• Set expectations in relation to governance, the risk assessment process, information security requirements, ICT operational management, security in the change and development processes and business continuity management to mitigate ICT and security risks. |
| | Monetary Authority of Singapore (MAS) - Guidelines on Risk Management Practices – Technology Risk (June 2013) | • Guidance on the oversight of technology risk management, security practices and controls to address technology risks. |
| | IAIS – Application Paper on the Use of Digital Technology in Inclusive Insurance (November 2018) | • Discusses digital technology applications in an inclusive insurance context and how the Insurance Core Principles can be applied in a proportionate manner in the supervision of the use of digital technologies in inclusive insurance. An Annex to the paper discusses the risks manifest in digital technology applications. |

| | | |
|---|---|---|
| FMI Resilience | The International Organization of Securities Commissions (IOSCO) Principles for Financial Market Infrastructures (PFMI) (April 2012) | • Ensure the security of critical functions and, in the event of a disruption, recovery of operational capacity in a timely manner.<br>• Require review of the entity's material risk exposure as a result of interdependencies with other entities.<br>• Require identification of events that prevent an entity from providing its critical operations and services as a going concern. |
| | Committee on Payments and Market Infrastructures (CPMI) & International Organization of Securities Commissions (IOSCO) - Guidance on Cyber Resilience for Financial Market Infrastructures (June 2016) | • Supplemental details, on top of the Principles for Financial Market Infrastructures (PFMI) [see row above], related to the preparations and measures that FMIs should undertake to enhance their cyber resilience capabilities with the objective of limiting the escalating risks that cyber threats pose to financial stability.<br>• Outlines five risk management categories that should be addressed across FMI's cyber resilience framework: governance; identification; protection; detection; and response and recovery. Also outlines three overarching components: testing; situational awareness; and learning and evolving. |
| Stress Testing | BCBS – Stress Testing Principles (October 2018) | • The principles are guidelines that focus on the core elements of stress testing frameworks. These include the objectives, governance, policies, processes, methodology, resources and documentation that guide stress testing activities and facilitate the use, implementation and oversight of stress testing frameworks. |
| | Bank of England - The Bank of England's approach to stress testing the UK banking system (October 2015) | • Stress tests therefore contribute to the Financial Policy Committee's statutory objective to protect and enhance the stability of the UK financial system, and, subject to that, support the economic policy of the Government. Equally, they contribute to the PRA's general objective to promote the safety and soundness of the banks it regulates, and its secondary objective to facilitate effective competition in the markets for services by the banks it regulates. |
| | Federal Review Board (FRB) - Comprehensive Capital Analysis and Review (CCAR) | • Ensure that banks have adequate capital to absorb losses and are able to lend to households and businesses even in a severe recession.<br>• Ensure that the largest and most systemically important financial institutions are able to continue to operate under severe economic stress conditions.<br>• Promote financial resilience that indirectly supports operational resilience by ensuring necessary resources to support operational capacity. |

| | | |
|---|---|---|
| | Federal Review Board (FRB) - Comprehensive Liquidity Analysis and Review (CLAR) | • Ensure the largest and most systemically important financial institutions' ability to continue to operate under severe liquidity stress.<br>• Require firms to assess the adequacy of their liquidity positions relative to their unique risks and tests the reliability of these institutions' approaches to managing liquidity risk.<br>• Promote financial resilience that indirectly supports operational resiliency by ensuring necessary resources to support operational capacity. |
| Recovery and Resolution | FSB - Guidance on Arrangements to Support Operational Continuity in Resolution (August 2016) | • Identify a number of arrangements including specific contractual provisions, access arrangements and governance structures that, if implemented appropriately, could support operational continuity in resolution. |
| | FSB - Key Attributes of Effective Resolution Regimes for Financial Institutions (October 2014) | • Set out core elements considered to be necessary for an effective resolution regime. |
| | FSB - Recovery and Resolution Planning for Systemically Important Financial Institutions: Guidance on Identification of Critical Functions and Critical Shared Services (July 2013) | • Provide basis for a strategic analysis that identifies firm's essential and systemically important (or "critical") functions.<br>• Assist evaluation of firm's criticality of functions.<br>• Promote common understanding of which functions and shared services are critical by providing shared definitions and evaluation criteria. |
| | European Commission - Bank Recovery and Resolution Directive (2014) | • Ensure continuity of bank's and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress and ii/ restoring viability of parts or all of the bank.<br>• Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers. |

| | | |
|---|---|---|
| | Bank of England (BoE) - Recovery and Resolution Planning (2013) | • Ensure continuity of bank's and maintaining financial stability by: i/ requiring banks to prepare recovery plans to overcome financial distress and ii/ restoring viability of parts or all of the bank.<br>• Grant national authorities powers to ensure an orderly resolution of failing banks with minimal costs for taxpayers. |
| | Federal Review Board (FRB) – Resolution Plan requirement under Regulation QQ (November 2011) | • Ensure the resilience and resolvability of globally systemic important banks (G-SIBs) without interruptions to the banks' critical operations and economic functions.... in a manner that substantially mitigates the risk that the failure of the bank would have serious adverse effects on financial stability |
| | IAIS – Application Paper on Recovery Planning (November 2019) | • Addresses governance, elements of a recovery plan and supervisory considerations, with an overarching focus on proportionality. The objective of a recovery plan should be to aid the insurer in understanding its own risks from a severe stress scenario and to be better prepared with an effective response and ensure timely activation and implementation of that response. |
| | FSB – Key Attributes Assessment Methodology for the Insurance Sector (August 2020) | • Provides a methodology for assessing the implementation of the Key Attributes of Effective Resolution Regimes for financial institutions in the insurance sector and applies to any insurer that could be systemically significant or critical if it fails (i.e. where the failure of the insurer could lead to a disruption of services critical for the functioning of the financial system or the real economy).<br>• The methodology is intended to be used primarily in assessments performed by authorities of the existing resolution regimes in their jurisdictions, in peer reviews and in IMF and World Bank assessments, including through Financial Sector Assessment Programs. |