DECEMBER 2024

RECOMMENDATIONS ON DCO SYSTEM SAFEGUARDS STANDARDS FOR THIRD PARTY SERVICE PROVIDERS

Report of the Technology and Operations Workstream of the Central Counterparty Risk and Governance ("CCP") Subcommittee, Market Risk Advisory Committee of the U.S. Commodity Futures Trading Commission (the "MRAC")

Commissioner Kristin N. Johnson, Sponsor of the MRAC

Alicia Crighton, Chair of the MRAC

This report was approved on November 25, 2024 by the CCP Risk and Governance Subcommittee of the MRAC. On December 10, 2024, the MRAC voted to approve distribution of this report to the U.S. Commodity Futures Trading Commission ("Commission" or "CFTC"). The views, analyses, and conclusions expressed herein reflect the work of the CCP Risk and Governance Subcommittee of the MRAC, and do not necessarily reflect the views of the MRAC, the Commission or its staff, the Federal Reserve Bank of Chicago, the Federal Reserve System, or the U.S. government. Reference to any products, services, websites, organizations, or enterprises, or the use of any organization, trade, firm, or corporation name is for informational purposes only and does not constitute endorsement, recommendation, or favoring by the U.S. government.

1. Background

1. Current DCO Rules, Form DCO, and Outsourcing.

1.1. Part 39.18 of the CFTC's regulations (System safeguards)

DCO Rule 18 currently imposes requirements with respect to outsourcing. DCO Rule 18 never expressly refers to a third-party relationship program. The outsourcing requirements are the following:

> *(d)* ***Outsourcing.***
>
> *(1) A derivatives clearing organization shall maintain the resources required under paragraphs (b)(4) and (c)(1) of this section either:*
>
> *(i) Using its own employees as personnel, and property that it owns, licenses, or leases; or*
>
> *(ii) Through written contractual arrangements with another derivatives clearing organization or other service provider.*
>
> *(2)* ***Retention of responsibility.*** *A derivatives clearing organization that enters into a contractual outsourcing arrangement shall retain complete responsibility for any failure to meet the requirements specified in paragraphs (b) and (c) of this section. The derivatives clearing organization must employ personnel with the expertise necessary to enable it to supervise the service provider's delivery of the services.*
>
> *(3)* ***Testing of resources.*** *The testing referred to in paragraph (e) of this section shall apply to all of the derivatives clearing organization's own and outsourced resources, and shall verify that all such resources will work together effectively. Where testing is required to be conducted by an independent contractor, the derivatives clearing organization shall engage a contractor that is independent from both the derivatives clearing organization and any outside service provider used to design, develop, or maintain the resources being tested.*[1]

Rule 18(d)(2) as currently worded expressly requires that the DCO "shall retain complete responsibility for any failure to meet the requirements" specified in Rule 18 with respect to outsourced services. The Rule also requires DCOs to "employ personnel with the expertise necessary to enable it to supervise the service provider's delivery of the services." Rule 18 (d)(3) also imposes testing requirements for outsourced resources.

1.2. CFTC Form DCO

Form DCO[2] requires a DCO to provide information to the Commission with respect to outsourced resources. In the instructions, Form DCO requires the following with respect to an outside service provider:

---

1 17 CFR 39.18.

2 Form DCO, Appendix A to 17 CFR part 39.

If Applicant intends to use the services of an outside service provider (including services of its clearing members or market participants), to enable Applicant to comply with any of the Core Principles, Applicant must submit as Exhibit A-10 all agreements entered into or to be entered into between Applicant and the outside service provider, and identify (1) the services that will be provided; (2) the staff of the outside service provider who will provide the services (specifying (i) in which department or unit of the outside service provider they are employed, (ii) title, and (iii) if know, level of expertise); and (3) the Core Principles addressed by such arrangement.

A statement identifying which resources are Applicant's own resources and which are provided by a service provider (outsourced). For resources that are outsourced, provide (i) all contracts governing the outsourcing arrangements, including all schedules and other supplemental materials, and (ii) a demonstration that Applicant employs personnel with the expertise necessary to enable them to supervise the service provider's delivery of the services. (b)(4)

An explanation of how Applicant will ensure the proper functioning of its systems, including its programs for the periodic objective testing and review of its systems and back-up facilities (including all of its own and outsourced resources), and verification that all such resources will work effectively together.

1.3. Annex F of the Principles for financial market infrastructures: Assessment methodology for the oversight expectations applicable to critical service providers[3]

Annex F of the Principles for financial market infrastructures addresses oversight expectations applicable to critical service providers of financial market infrastructures (FMIs), recognizing that each FMI remains ultimately responsible for its operations. The CCP Risk and Governance Subcommittee of MRAC recommends that the Commission consider requiring DCOs to obtain assurance from their critical service providers that they comply with the expectations set forth in Annex F of the PFMI, which is attached as an Exhibit to this Report.

2. Recommendation and Discussion

2.1. Recommended Scope and Substance of the Proposed Rulemaking

It is recommended that the proposed regulation build upon and incorporate the language, concepts and principles already set out in the System Safeguards Rule found in Part 39.18 of the CFTC's regulations (Rule 18-System safeguards)[4] with respect to DCO. The proposed regulation would further require that each DCO establish, implement, and maintain a Third-Party

[3] PFMI Assessment methodology for the oversight expectations applicable to critical services providers (published December 2014 by Committee on Payments and Market Infrastructures and Board of the International Organization of Securities Commissions), https://www.bis.org/cpmi/publ/d123.pdf.

[4] System Safeguards, 17 CFR 39.18.

Relationship Management Program (a "TPMP")[5] beyond what is currently in the Rule 18-System Safeguards

We recommend that the Commission take a principles-based approach by adding TPMP principles to current Rule 18 (2). These principles are intended to reflect lessons learned from industry efforts and best practices in derivatives, the guidance notes in Form DCO, the NFA interpretive guidance, lessons learned from the wider context of third-party relationship management, as well as the principles enunciated in the PFMIs. Incorporating these principles in Commission regulations would enable the Commission to update its regulatory framework with respect to critical third party service providers and to bring its regulations in line with internationally accepted standards, while maintaining a principles based approach to regulation.

2.2 Recommended amendment to Rule 18:

Workstream participants recommend that the Commission amend

(2) ***Retention of responsibility.*** *A derivatives clearing organization that enters into a contractual outsourcing arrangement shall retain complete responsibility for any failure to meet the requirements specified in paragraphs (b) and (c) of this section. The derivatives clearing organization must employ personnel with the expertise necessary to enable it to supervise the service provider's delivery of the services.*

A DCO shall retain responsibility over critical third-party arrangements provided by Third Party Service Providers (TPSP) by establishing a robust Third-Party Risk Management Program (TPRM). A robust TPRM program should identify, assess, mitigate and monitor the full scope of risks that the use of third party arrangements through implementation, at a minimum, of the following principles:

A DCO should:

a. Implement written policies and procedures reasonably designed to cover the entire lifecycle[6] of the third party service relationship and to manage risks associated with Third Party arrangements.
b. Employ personnel with the expertise necessary to enable the DCO to monitor and supervise TPSP's performance against contractual requirements.
c. Conduct a pre-selection and an onboarding due diligence assessment, before entering into any third party service arrangement, of the impact to the DCO's operational risk, including an assessment of the TPSP's financial posture, insurance coverage, contingency plans.
d. Establish written policies and procedures to determine which of a DCO's TPSPs are Critical TPSPs (CTPSPs) considering the following:

---

[5] The concept of "operational resilience" can be broadly understood as the ability of an organization to resist, absorb, and recover from disruption or harm to mission-critical functions. *See*, *e.g.*, NIST SP 800-160 Vol. 2 Rev. 1 from CNSSI 4009-2015.

[6] The lifecycle of a third-party service relationship typically includes planning, due diligence and selection of a service provider, contracting, ongoing monitoring, and termination.

i. dependencies on functionality or support which would have a material impact on CFTC regulated activities if unavailable or if the service is impaired;
ii. impact to critical operations or firm viability;
iii. material impact on the ability to meet key legal and regulatory obligations;
iv. significant customer impact;
v. potential significant security risks (including cybersecurity);
vi. risk of concentration of third-party providers that the DCO has an arrangement with; and

e. exit strategy and alternative solutions. With respect to CTPSPs, apply enhanced risk based due diligence and oversight to critical services.
f. Establish written policies and procedures to perform ongoing risk-based monitoring of performance of each CTPSP, based on generally accepted industry standards.
g. Maintain adequate records of the agreements between the DCO and each CTPSP, each such agreement identifying (1) the scope of services that will be provided; (2) applicable services level agreements (SLAs); (3) contact at the CTPSP; and termination provisions.
h. Establish reasonable standards for offboarding/ termination of CTPSPs.

Exhibit

Annex F of the PFMI[7]

Annex F: Oversight expectations applicable to critical service providers

The operational reliability of an FMI may be dependent on the continuous and adequate functioning of service providers that are critical to an FMI's operations, such as information technology and messaging providers. A regulator, supervisor, or overseer of an FMI may want to establish expectations for an FMI's critical service providers in order to support the FMI's overall safety and efficiency. The expectations should help ensure the operations of a critical service provider are held to the same standards as if the FMI provided the service. The expectations outlined below are specifically targeted at critical service providers and cover risk identification and management, robust information security management, reliability and resilience, effective technology planning, and strong communications with users. These expectations are written at a broad level, allowing critical service providers flexibility in demonstrating that they meet the expectations.

1.Risk identification and management: **A critical service provider is expected to identify and manage relevant operational and financial risks to its critical services and ensure that its risk-management processes are effective.**

A critical service provider should have effective processes and systems for identifying and documenting risks, implementing controls to manage risks, and making decisions to accept certain risks. A critical service provider may face risks related to information security, reliability and resilience, and technology planning, as well as legal and regulatory requirements pertaining to its corporate organization and conduct, relationships with customers, strategic decisions that affect its ability to operate as a going concern, and dependencies on third parties. A critical service provider should reassess its risks, as well as the adequacy of its risk-management framework in addressing the identified risks, on an ongoing basis. The identification and management of risks should be overseen by the critical service provider's board of directors (board) and assessed by an independent, internal audit function that can communicate clearly its assessments to relevant board members. The board is expected to ensure an independent and professional internal audit function. The internal audit function should be reviewed to ensure it adheres to the principles of a professional organization that governs audit practice and behaviour (such as the Institute of Internal Auditors) and is able to independently assess inherent risks as well as the design and effectiveness of risk-management processes and internal controls. The internal audit function should also ensure that its assessments are communicated clearly to relevant board members.

2.Information security: A critical service provider is expected to implement and maintain appropriate policies and procedures, and devote sufficient resources to ensure the confidentiality and integrity of information and the availability of its critical services in order to fulfil the terms of its relationship with an FMI.

A critical service provider should have a robust information security framework that appropriately manages its information security risks. The framework should include sound policies and procedures to protect information from unauthorised disclosure, ensure data integrity, and guarantee the availability of its services. In addition, a critical service provider should have policies and procedures for monitoring its compliance with its information security framework. 170 CPSS-

[7] Annex F, at 170, https://www.bis.org/cpmi/publ/d123.htm.

IOSCO – Principles for financial market infrastructures – April 2012 This framework should also include capacity planning policies and change-management practices. For example, a critical service provider that plans to change its operations should assess the implications of such a change on its information security arrangements.

3.Reliability and resilience: A critical service provider is expected to implement appropriate policies and procedures, and devote sufficient resources to ensure that its critical services are available, reliable, and resilient. Its business continuity management and disaster recovery plans should therefore support the timely resumption of its critical services in the event of an outage so that the service provided fulfils the terms of its agreement with an FMI.

A critical service provider should ensure that it provides reliable and resilient operations to users, whether these operations are provided to an FMI directly or to both an FMI and its participants. A critical service provider should have robust operations that meet or exceed the needs of the FMI. Any operational incidents should be recorded and reported to the FMI and the FMI's regulator, supervisor, or overseer. Incidents should be analysed promptly by the critical service provider in order to prevent recurrences that could have greater implications. In addition, a critical service provider should have robust business continuity and disaster recovery objectives and plans. These plans should include routine business continuity testing and a review of these test results to assess the risk of a major operational disruption.

4.Technology planning: The critical provider is expected to have in place robust methods to plan for the entire lifecycle of the use of technologies and the selection of technological standards.

A critical service provider should have effective technology planning that minimises overall operational risk and enhances operational performance. Planning entails a comprehensive information technology strategy that considers the entire lifecycle for the use of technologies and a process for selecting standards when deploying and managing a service. Proposed changes to a critical service provider's technology should entail a thorough and comprehensive consultation with the FMI and, where relevant, its participants. A critical service provider should regularly review its technology plans, including assessments of its technologies and the processes it uses for implementing change.

5.Communication with users: A critical service provider is expected to be transparent to its users and provide them sufficient information to enable users to understand clearly their roles and responsibilities in managing risks related to their use of a critical service provider.

A critical service provider should have effective customer communication procedures and processes. In particular, a critical service provider should provide the FMI and, where appropriate, its participants with sufficient information so that users clearly understand their roles and responsibilities, enabling them to manage adequately their risks related to their use of the services provided. Useful information for users typically includes, but is not limited to, information concerning the critical service provider's management processes, controls, and independent reviews of the effectiveness of these processes and controls. As a part of its communication procedures and processes, a critical service provider should have mechanisms to consult with users and the broader market on any technical changes to its operations that may affect its risk profile, including incidences of absent or non-performing risk controls of services. In addition, a

critical service provider should have a crisis communication plan to handle operational disruptions to its services.

Members of the MRAC CCP Risk and Governance Subcommittee

Alessandro Cocco (Chair)	Federal Reserve Bank of Chicago, on detail at the Department of the Treasury	Senior Policy Advisor
Alicia Crighton	Futures Industry Association	Global Co-Head of Futures and Head of OTC and Prime Clearing Businesses, Goldman Sachs
Ruth Arnould	Bank of America	Managing Director and Associate General Counsel
Richard Berner	New York University	Clinical Professor of Management Practice in the Department of Finance and Co-Director of the Stern Volatility and Risk Institute
Lee Betsill	CME Group	Managing Director and Chief Risk Officer
Juan Blackwell	Ontario Teachers' Pension Plan	Head of Credit & Counterparty Risk Management
Joseph Garelick	BlackRock	Vice President of Risk & Quantitative Analysis Group
Reginald Griffith	Louis Dreyfus Company	Global Head of Regulatory Compliance
Graham Harper	Futures Industry Association – Principal Traders Group	Head of Public Policy and Market Structure at DRW
David Horner	London Stock Exchange Group	Chief Risk Officer, LCH Ltd
Demetri Karousos	Nodal Exchange, LLC	President and COO
Elizabeth King	Intercontinental Exchange	Global Head of Clearing and Chief Regulatory Officer
Tim McHenry	National Futures Association	Senior Vice President

Rajalakshmi Ramanath	J.P. Morgan	Executive Director, CCP Credit and Risk Strategy
Paolo Saguato	George Mason University	Associate Professor of Law, Antonin Scalia Law School
Dmitrij Senko	Eurex Clearing AG	Chief Risk Officer
Viktor Vadasz	Morgan Stanley	Executive Director, Bank Resource Management