# Deloitte.

# **CFTC** proposes operational resilience framework



The Commodity Futures Trading Commission (CFTC) proposed a rule requiring firms to establish an **Operational Resilience Framework (ORF)** to manage and monitor Operational Risk amidst rising cyberattacks. The rule applies to **Futures Commission Merchants (FCMs)**, **Swap Dealers (SDs)**, and **Major Swap Participants (MSPs)**, collectively referred to as "Covered Entities". It necessitates changes to certain elements of operational risk frameworks and a review or refinement of risk management practices.

#### **Summary requirements**

#### Information and technology security program requirements:

- Perform annual risk assessments with oversight by designated officer or supervisory body
- · Establish internal controls reasonably designed to prevent, detect, and mitigate identified risks
- Develop a written incident response plan, standalone or part of business continuity plan

#### Third-party relationship program (TPRP) requirements:

- Address risk at all stages of the third-party relationship lifecycle (5 stages: i.e., preselection, duediligence, negotiations, monitoring, and termination)
- Maintain a current inventory of third-party service providers
- Perform heightened due diligence and ongoing monitoring for vendors identified as "critical thirdparty service providers"

#### Business continuity and disaster recovery (BC-DR) plan requirements:

- Adopt processes that help identify all covered information & data required by regulation
- · Resume operation as soon as reasonably possible without adhering to 'next business day' clause
- · Diversify resources to prevent one emergency incident from affecting multiple processes/systems

#### Reporting of important notifications requirements:

- Notify the CFTC of any incidents affecting information and technology security, business continuity, and customer assets or positions
- Alert the CFTC within 24 hours of a covered BC-DR activation following an incident
- Notify customers and counterparties of any incidents affecting their interests

#### Testing and review of ORF requirements:

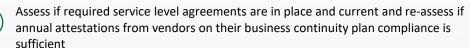
- Conduct testing of the operation risk framework dictated by the nature, size, scope, complexity, and risk profile of business activities
- Perform annual testing of IT security program, incident response plan and BCDR plan
- Implement process for review and annual attestation by the senior officer or oversight body

#### <sup>1</sup> CFTC, Operational Resilience Framework, 2024.

#### **Call to Action for Covered Entities**

While Covered Entities generally operate with Vendor Management and Business Continuity programs, as well as Information Security capabilities, the 'Call to Action' includes the following:

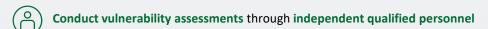








Revisit testing of incident response plan and recovery time frames to determine if plan has been tested sufficiently, and tests executed yield appropriate results



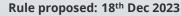
Test the effectiveness of backup facilities, capabilities and turnaround timeframes

Provide incident reporting, notifications management and escalation protocol for exceeding risk tolerance levels within 24 hours of the risk event

Employ conscientious data protection measures such as backups, encryption, and access controls.

Explore and leverage technology innovations such as automation and AI to bolster operational risk management practices







Comments: 1st April 2024

# **Deloitte**



### **Connect with us**

## Marjorie Forestal

Principal | Deloitte & Touche LLP mforestal@deloitte.com

## Momtaz Yaqubie

Manager | Deloitte & Touche LLP myaqubie@deloitte.com

### Nathan Freeman

Manager | Deloitte & Touche LLP nafreeman@deloitte.com

### Meghan Burns

Manager | Deloitte & Touche LP megburns@deloitte.com

### Kumar, Amitam

Senior Solution Manager | Deloitte & Touche Assurance & Enterprise Risk Services India Private Limited <a href="mailto:amitakumar@deloitte.com">amitakumar@deloitte.com</a>

## Alex Pape

Senior Consultant | Deloitte & Touche LLP alepape@deloitte.com

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.