SECURITIES AND EXCHANGE COMMISSION
(Release No. 34-81745; File Nos. SR-DTC-2017-014; SR-NSCC-2017-013; SR-FICC-2017-017)

September 28, 2017

Self-Regulatory Organizations; The Depository Trust Company; National Securities Clearing Corporation; Fixed Income Clearing Corporation; Order Approving Proposed Rule Changes to Adopt the Clearing Agency Operational Risk Management Framework

I. Introduction

On July 25, 2017, The Depository Trust Company ("DTC"), Fixed Income Clearing Corporation ("FICC"), and National Securities Clearing Corporation ("NSCC," each a "Clearing Agency," and collectively with DTC and FICC, the "Clearing Agencies"), filed with the Securities and Exchange Commission ("Commission") proposed rule changes SR-DTC-2017-014, SR-NSCC-2017-013, and SR-FICC-2017-017, respectively, pursuant to Section 19(b)(1) of the Securities Exchange Act of 1934 ("Act")[1] and Rule 19b-4 thereunder.[2] The proposed rule changes were published for comment in the Federal Register on August 14, 2017.[3] The Commission did not receive any comment letters on the proposed rule changes. For the reasons discussed below, the Commission approves the proposed rule changes.

II. Description of the Proposed Rule Changes

The proposed rule changes would adopt the Clearing Agency Operational Risk Management Framework ("Framework") of the Clearing Agencies, as described below.

---

1 15 U.S.C. 78s(b)(1).

2 17 CFR 240.19b-4.

3 Securities Exchange Act Release No. 81338 (August 8, 2017), 82 FR 36049 (August 14, 2017) (SR-DTC-2017-014, SR-NSCC-2017-013, SR-FICC-2017-017) ("Notice").

A. Overview of the Framework

The Framework would describe how each of Clearing Agency manages operational risk. Operational risk is defined by the Clearing Agencies in the Framework as the risk of direct or indirect loss or reputational harm resulting from an event, internal or external, that is the result of inadequate or failed processes, people, and systems ("Operational Risk").[4] More specifically, the Framework would describe how the Clearing Agencies (i) manage Operational Risk; (ii) manage their information technology risks; and (iii) manage their business continuity risks.[5] The DTCC Operational Risk Management group ("ORM") would maintain the Framework, on behalf of the Clearing Agencies.[6]

B. Operational Risk Management

The Framework would describe how ORM is charged with establishing appropriate systems, policies, procedures, and controls to enable the Clearing Agencies to identify plausible sources of Operational Risk.[7]

---

4 Notice, 82 FR at 37943.

5 Id.

6 Id. The parent company of the Clearing Agencies is The Depository Trust & Clearing Corporation ("DTCC"). DTCC operates on a shared services model with respect to the Clearing Agencies. Most corporate functions are established and managed on an enterprise-wide basis pursuant to intercompany agreements under which it is generally DTCC that provides a relevant service to a Clearing Agency.

7 Notice, 82 FR at 37943.

Specifically, the Framework would describe how the Clearing Agencies identify key risks, including Operational Risk, and set metrics to categorize such risks (e.g., from "no impact" to "severe impact") through "Risk Tolerance Statements."[8] The Framework would describe how the Risk Tolerance Statements identify the overall risk reduction or mitigation objectives of the Clearing Agencies, with respect to identified risks to the Clearing Agencies.[9] The Framework would also explain how the Risk Tolerance Statements document the risk controls and other measures the Clearing Agencies would use to manage such identified risks (including escalation requirements in the event of risk metric breaches). The Framework would state that ORM would annually review, revise, update, and/or create, as necessary, each Risk Tolerance Statement.[10]

The Framework would also describe how the Clearing Agencies monitor key risks, including Operational Risk, through "Risk Profiles."[11] The Framework would state that "Risk Profiles" identify how risk is assessed for each of the Clearing Agencies' businesses and support areas (each a "Clearing Agency Business" and/or "Clearing Agency Support Area").[12] The Framework would explain that the risk assessment documented in these profiles includes (1) assessment of inherent risk (i.e., risk without any mitigating controls); (2) evaluation of existing controls and, as appropriate, any new additional controls, as well as the evaluation of the same risk against the strength of such controls; and (3) identification of any residual risk and a

---

8 Id.

9 Id.

10 Id.

11 Id.

12 Id.

determination to either further mitigate such risk or accept such risk by the applicable Clearing Agency Business or Clearing Agency Support Area.[13]

The Framework would then describe generally the responsibilities of ORM, which is part of the second line of defense within the Clearing Agencies' "Three Lines of Defense" approach to risk management.[14] The Framework would identify ORM responsibilities including, but not limited to, management of the Risk Tolerance Statements, and working with the Clearing Agency Businesses and Clearing Agency Support Areas to create and monitor Risk Profiles. [15]

C. Information Technology Risks

The Framework would describe how the Clearing Agencies address information technology risks.[16] The Framework would state that the DTCC Technology Risk Management group ("TRM"), on behalf of the Clearing Agencies, is responsible for establishing appropriate programs, policies, procedures, and controls with respect to the Clearing Agencies' information technology risks.[17] The Framework would indicate that these responsibilities would help respective Clearing Agency's management to ensure that systems have a high degree of security,

---

13 Id.

14 Id. The Three Lines of Defense approach to risk management identifies the roles and responsibilities of different Clearing Agency Businesses or Clearing Agency Support Areas in identifying, assessing, measuring, monitoring, mitigating, and reporting certain key risks faced by the Clearing Agencies. The Three Lines of Defense approach is more fully described in a separate framework, the Clearing Agency Risk Management Framework. See Securities Exchange Act Release No. 81635 (September 15, 2017), 82 FR 44224 (September 21, 2017)(SR-DTC-2017-013, SR-NSCC-2017-012, SR-FICC-2017-016).

15 Notice, 82 FR at 37943.

16 Id.

17 Id.

resiliency, operational reliability, and adequate, scalable capacity.[18] The Framework would describe some of the recognized information technology standards that TRM may use to execute its responsibilities (as applicable).[19]

The Framework would also identify some of TRM's responsibilities, including (1) performing risk assessments to, among other things, facilitate the determination of the Clearing Agencies' investment and remediation priorities; (2) facilitating annual mandatory and periodic information security awareness, education, training, and communication to personnel of Clearing Agency Businesses and Clearing Agency Support Areas and relevant external parties; and (3) creating, implementing, and managing certain programs, including programs that (i) address information security throughout a system's lifecycle, (ii) facilitate compliance with evolving and established regulatory rules and guidelines that govern protection of the information assets of the Clearing Agencies and their participants, (iii) identify, prioritize, and manage the level of cyber threats to the Clearing Agencies, and (iv) assure that access to Clearing Agency information assets is appropriately authorized and authenticated based on current business need.[20]

Additionally, the Framework would note that TRM's risk strategy is closely aligned to the Clearing Agencies' business drivers and future strategic direction.[21] The Framework would state that such risk strategy allows the Clearing Agencies to achieve information security threat mitigation objectives, resiliency of infrastructure supporting Clearing Agency critical business

---

18 Id.

19 Id.

20 Id.

21 Id.

applications, and operational reliability.[22] The Framework would also describe how TRM's early and consistent involvement in initiatives to develop new products and systems establishes this priority.[23] The Framework would state that TRM is involved from the initial planning phase through the design, build, and operative phases of those initiatives, to address certain requirements.[24] The Framework would then explain that TRM's involvement specifically addresses effectiveness, reliability, and availability requirements of those initiatives, incorporating those requirements into the initiatives' design and execution (from both a technology and cyber security perspective).[25]

The Framework would next describe the Clearing Agencies' security strategy and defense, stating that the Clearing Agencies' network security framework and preventive controls are designed to support a reliable and robust tiered security strategy and defense.[26] The Framework would state that these controls include modern and technically advanced security firewalls, intrusion detection, system and data monitoring, and data protection tools.[27] The Framework would also describe the Clearing Agencies' enhanced security features and the standards they use to assess vulnerabilities and potential threats.[28]

---

22 Notice, 82 FR at 37943-44.

23 Notice, 82 FR at 37944.

24 Id.

25 Id.

26 Id.

27 Id.

28 Id.

D. Business Continuity Risks

Finally, the Framework would describe how the Clearing Agencies establish and maintain business continuity plans to address events that may pose significant business continuity risks (i.e., disrupting of Clearing Agency operations).[29] The Framework would identify how the business continuity process for each Clearing Agency Business and Clearing Agency Support Area is ranked by the significance of a possible disruption to its operation.[30] The Framework would explain that these rankings fall within a range of tiers, from 0 to 5, based on criticality to each applicable Clearing Agency's operations (each a "Tier"), where Tier 0 equates to critical operations or support of such operations for which virtually no downtime is permitted under applicable regulatory standards, and Tier 5 equates to non-essential operations or support of such operations for which recovery times of greater than five days is permitted.[31]

The Framework would state that each Clearing Agency Business and Clearing Agency Support Area annually updates its own business continuity plan, as well as reviews and ratifies its business impact analysis.[32] The Framework would describe that the DTCC Business Continuity Management department ("BCM") uses that analysis, on behalf of the Clearing Agencies, to validate the Business' or Support Area's current Tier ranking, described above.[33] The Framework would identify the key elements of the business impact analysis, including (1) an assessment of the criticality of the applicable Clearing Agency Business or Clearing Agency

---

29 Id.

30 Id.

31 Id.

32 Id.

33 Id.

Support Area, based on potential impact to the Clearing Agency; (2) an estimation of the maximum allowable downtime for the applicable Clearing Agency Business or Clearing Agency Support Area; and (3) the identification of dependencies, and the ranking of such dependencies to align with the criticality of the applicable Clearing Agency Business's, or Clearing Agency Support Area's, recovery.[34]

The Framework would describe the Clearing Agencies' multiple data centers, and the emergency monitoring and back-up systems available at each site.[35] The Framework would explain the capacity of the various data centers (including emergency monitoring and back-up systems).[36] The Framework would also describe how the Clearing Agencies' operating centers (which may include data centers) assist in recovery efforts, and explain how each Clearing Agency Business and Clearing Agency Support Area creates and deploys its own work-area recovery strategy to mitigate the loss of primary workspace and/or associated desktop technology, as well as for purposes of appropriately locating personnel.[37] The Framework would further indicate how each work-area recovery strategy is developed and executed (based on the applicable Clearing Agency Business' and Clearing Agency Support Area's current Tier ranking, as described above).[38]

---

34 Id.

35 Id.

36 Id.

37 Id.

38 Id.

The Framework would describe the responsibilities of BCM in managing a disruptive business event.[39] The Framework would state that managing a disruptive business event would include coordination with a team of representatives from each Clearing Agency Business and Clearing Agency Support Area.[40] Finally, the Framework would describe how the Clearing Agencies conduct regular exercises used to simulate loss of Clearing Agency locations, and would describe some of the preventive measures the Clearing Agencies take with respect to business continuity risk management.[41]

III. Discussion and Commission Findings

Section 19(b)(2)(C) of the Act directs the Commission to approve a proposed rule change of a self-regulatory organization if it finds that such proposed rule change is consistent with the requirements of the Act and rules and regulations thereunder applicable to such organization.[42] After carefully considering the proposed rule changes, the Commission finds that the proposed rule changes are consistent with the requirements of the Act and the rules and regulations thereunder applicable to the Clearing Agencies. Specifically, the Commission finds that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act[43] and Rules 17Ad-22(e)(17)(i)–(iii) under the Act.[44]

---

39 Id.

40 Id.

41 Id.

42 15 U.S.C. 78s(b)(2)(C).

43 15 U.S.C. 78q-1(b)(3)(F).

44 17 CFR 240.17Ad-22(e)(17)(i)-(iii).

A. Consistency with Section 17A(b)(3)(F) of the Act

Section 17A(b)(3)(F) of the Act requires, in part, that the rules of a registered clearing agency be designed to assure the safeguarding of securities and funds which are in the custody or control of the Clearing Agencies or for which they are responsible.[45]

As described above, the Framework would describe how the Clearing Agencies manage their Operational Risk. Specifically, the Frameworks would describe how the Clearing Agencies address their technology risks, information security risks, and their business continuity risks. The Framework would describe the processes, systems, and controls (as well as the supporting policies and procedures) used by the Clearing Agencies to identify, manage, and mitigate risks which threaten the Clearing Agencies' ability to function.

By describing their Operational Risk practices in a clear and comprehensive manner, the Framework is designed to help the Clearing Agencies prevent and manage the risks that arise in, or are borne by, the Clearing Agencies. The Framework would explain how the Clearing Agencies identify and mitigate risks generally (through the Three Lines of Defense, Risk Tolerance Statements, and Risk Profiles), as well as how they specially identify and mitigate information technology risk (through the TRM's efforts) and business continuity risk (through data centers and operational centers). By better managing the risks that arise in or are bone by the Clearing Agencies through such risk mitigation practices, the Framework is designed to help reduce the possibility that a Clearing Agency fails. By better positioning the Clearing Agencies to continue their critical operations and services, and mitigating the risk of financial loss contagion caused by a Clearing Agency failure, the Framework is designed to help assure the safeguarding of securities and funds which are in the custody or control of the Clearing

[45] 15 U.S.C. 78q-1(b)(3)(F).

Agencies, or for which they are responsible. Accordingly, the Commission believes that the proposed rule changes are consistent with Section 17A(b)(3)(F) of the Act.[46]

B. Consistency with Rule 17Ad-22(e)(17)(i)

Rule 17Ad-22(e)(17)(i) under the Act requires, in part, that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by identifying the plausible sources of operational risk, both internal and external, and mitigating their impact through the use of appropriate systems, policies, procedures, and controls.[47]

As described above, the Framework would describe how the Risk Tolerance Statements and the Risk Profiles assist the Clearing Agencies identify and mitigate the plausible sources of Operational Risk, both internal and external. As described above, the Framework explains how the Risk Tolerance Statements (i) identify both internal and external Clearing Agency risks; (ii) categorize the respective Clearing Agencies' tolerance for those risks; and (iii) then identify governance process applicable to any breach of those tolerances. In this way, the Risk Tolerance Statements are designed to help the Clearing Agencies to identify and manage the internal and external risks. As also described above, the Framework would describe how the Risk Profiles are designed to serve a similar function, by serving as a tool for identifying and assessing inherent risks, and evaluating the controls around those risks. The Framework also describes the role of ORM, which includes oversight of both the Risk Tolerance Statements and Risk Profiles.

By describing the functions of the Risk Tolerance Statements and Risk Profiles, (which, together, are designed to (i) assist the Clearing Agencies in effectively managing their

---

46 Id.

47 17 CFR 240.17Ad-22(e)(17)(i).

operational risks by identifying the plausible sources of operational risk, both internal and external, and (ii) assist the Clearing Agencies in mitigating the impact of those risks), and by describing the role of ORM in overseeing the Risk Tolerance Statements and Risk Profiles, the Commission believes the Framework is consistent with the requirements of Rule 17Ad-22(e)(17)(i).[48]

C. Consistency with Rule 17Ad-22(e)(17)(ii)

Rule 17Ad-22(e)(17)(ii) under the Act requires, in part, that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by ensuring that systems have a high degree of security, resiliency, operational reliability, and adequate, scalable capacity.[49]

As noted above, the Framework would describe how the Clearing Agencies manage their Operational Risk. Specifically, the Framework would describe TRM's role and responsibilities in managing the Clearing Agencies' information technology risks. In particular, the Framework would identify TRM's (i) programs, systems, and controls; (ii) information technology risk management standards; and (iii) continuous role in product and project initiatives to address security issues through the lifecycle of Clearing Agency initiatives.

The Framework thereby describes how TRM is designed to safeguard the integrity of the Clearing Agencies' information technology, as well as the standards against which TRM's safeguards would be evaluated. In this manner, the Framework is designed to ensure that the Clearing Agencies' systems have a high degree of security, resiliency, and operational reliability. Furthermore, as the Framework indicates TRM's early and continuous involvement in the

---

48 Id.

49 17 CFR 240.17Ad-22(e)(17)(ii).

Clearing Agencies' initiatives, the Framework reveals how TRM would enable the Clearing Agencies to grow and evolve while accounting for technology and cyber security concerns, thereby ensuring the Clearing Agencies' adequate and scalable capacity.

Therefore, by describing TRM's role and responsibilities in helping the Clearing Agencies maintain systems with a high degree of security, resiliency, operational reliability, and adequate, scalable capacity, the Commission believes the Framework is consistent with the requirements of Rule 17Ad-22(e)(17)(ii).[50]

D. Consistency with Rule 17Ad-22(e)(17)(iii)

Rule 17Ad-22(e)(17)(iii) under the Act requires, in part, that each covered clearing agency establish, implement, maintain and enforce written policies and procedures reasonably designed to manage the covered clearing agency's operational risks by establishing and maintaining a business continuity plan that addresses events posing a significant risk of disrupting operations.[51]

As described above, the Framework would describe how the Clearing Agencies establish and maintain business continuity plans. Specifically, the Framework would describe the critical features of the Clearing Agencies' business continuity plans to demonstrate how they are designed to address events posing a significant risk of disrupting the Clearing Agencies' operations. The Framework would also indicate how each Clearing Agency Business and Clearing Agency Support Area reviews and ratifies its respective plan and its business impact analysis, relative to its assigned Tier. Therefore, as the Framework describes how the Clearing Agencies establish and maintain their business continuity plans, which are designed to address

---

50 Id.

51 17 CFR 240.17Ad-22(e)(17)(iii).

events posing a significant risk of disrupting operations, the Commission believes that the Framework is consistent with the requirements of Rule 17Ad-22(e)(17)(iii).[52]

IV. Conclusion

On the basis of the foregoing, the Commission finds that the proposed rule changes are consistent with the requirements of the Act and in particular with the requirements of Section 17A of the Act[53] and the rules and regulations thereunder.

IT IS THEREFORE ORDERED, pursuant to Section 19(b)(2) of the Act, that proposed rule changes SR-DTC-2017-014, SR-NSCC-2017-013, and SR-FICC-2017-017 be, and hereby are, APPROVED.[54]

For the Commission, by the Division of Trading and Markets, pursuant to delegated authority.[55]

Eduardo A. Aleman
Assistant Secretary

---

52 Id.

53 15 U.S.C. 78q-1.

54 In approving the Proposed Rule Changes, the Commission considered the proposals' impact on efficiency, competition and capital formation. 15 U.S.C. 78c(f).

55 17 CFR 200.30-3(a)(12).