FEDERAL RESERVE SYSTEM

12 CFR Part 234

Regulation HH; Docket No. R-1782

RIN No. 7100-AG40

Financial Market Utilities

AGENCY: Board of Governors of the Federal Reserve System

ACTION: Final rule

SUMMARY: The Board of Governors of the Federal Reserve System (Board) is publishing a final rule amending the requirements relating to operational risk management in the Board's Regulation HH, which applies to certain financial market utilities (FMUs) that have been designated as systemically important (designated FMUs) by the Financial Stability Oversight Council (FSOC) under Title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (the Dodd-Frank Act or Act). The amendments update, refine, and add specificity to the operational risk management requirements in Regulation HH to reflect changes in the operational risk, technology, and regulatory landscape in which designated FMUs operate. The final rule also adopts specific incident-notification requirements.

DATES: *Effective Date:* The final rule is effective **[INSERT DATE THAT IS 30 DAYS AFTER PUBLICATION IN THE FEDERAL REGISTER]**.

Compliance Dates: Designated FMUs must be in compliance with the rule by [INSERT DATE THAT IS 180 DAYS AFTER PUBLICATION], except for the incident management and notification requirement in § 234.3(a)(17)(vi), under Amendatory Instruction 3, with which designated FMUs must be in compliance by [INSERT DATE THAT IS 90 DAYS AFTER PUBLICATION].

FOR FURTHER INFORMATION CONTACT: Emily Caron, Assistant Director (202-452-5261) or Katherine Standbridge, Senior Financial Institution and Policy Analyst (202-452-3873), Division of Reserve Bank Operations and Payment Systems; or Corinne Milliken Van Ness, Senior Counsel (202-452-2421) or M. Benjamin Snodgrass, Senior Counsel (202-263-4877), Legal Division. For users of TTY-TRS, please call 711 from any telephone, anywhere in the United States.

SUPPLEMENTARY INFORMATION:

I. Overview

Title VIII of the Dodd-Frank Act, titled the "Payment, Clearing, and Settlement Supervision Act of 2010," was enacted to mitigate systemic risk in the financial system and to promote financial stability, in part, through an enhanced supervisory framework for designated FMUs. Section 803(6) of the Act defines an FMU as a "person that manages or operates a multilateral system for the purpose of transferring, clearing, or settling payments, securities, or other financial transactions among financial institutions or between financial institutions and the person."[1] Pursuant to section 805(a)(1)(A) of the Act, and as described below, the Board is required to prescribe risk-management standards governing the operations related to the payment, clearing, and settlement activities of certain designated FMUs.

The Board adopted Regulation HH, Designated Financial Market Utilities, in July 2012 to implement, among other things, the statutory provisions under section 805(a)(1)(A) of the

[1] 12 U.S.C. 5462(6).

Act.[2] In November 2014, the Board published amendments to the risk-management standards in Regulation HH based on the *Principles for Financial Market Infrastructures* (PFMI).[3]

In October 2022, the Board published for comment a notice of proposed rulemaking (NPRM) to amend the requirements relating to operational risk management in Regulation HH. The Board proposed to update, refine, and add specificity to the operational risk management requirements in Regulation HH. The proposed amendments reflected changes in the operational risk, technology, and regulatory landscape in which designated FMUs operate since the Board last amended Regulation HH in 2014. The Board also proposed to adopt specific incident-notification requirements.[4] The public comment period for the proposed amendments closed on December 5, 2022. The Board is now adopting final amendments to Regulation HH, with modifications to certain sections of the proposal as discussed below.

II. Background

A. Financial Market Utilities

FMUs provide essential infrastructure to clear and settle payments and other financial transactions. Financial institutions, including banking organizations, participate in FMU arrangements pursuant to a common set of rules and procedures, technical infrastructure, and risk-management framework.

---

[2] 77 FR 45907 (Aug. 2, 2012).

[3] 79 FR 65543 (Nov. 5, 2014). The PFMI, published by the Committee on Payment and Settlement Systems (now the Committee on Payments and Market Infrastructures) and the Technical Committee of the International Organization of Securities Commissions in April 2012, is widely recognized as the most relevant set of international risk-management standards for payment, clearing, and settlement systems.

[4] 87 FR 60314 (Oct. 5, 2022).

If a systemically important FMU fails to perform as expected or fails to effectively measure, monitor, and manage its risks, it could pose significant risk to its participants and the financial system more broadly. For example, the inability of an FMU to complete settlement on time could create credit or liquidity problems for its participants or other FMUs. An FMU, therefore, should have a robust risk-management framework, including appropriate policies and procedures to measure, monitor, and manage the range of risks that arise in or are borne by the FMU.

B. Title VIII of the Dodd-Frank Act

In recognition of the criticality of FMUs to the stability of the financial system, Title VIII of the Dodd-Frank Act established a framework for enhanced supervision of certain FMUs. Section 804 of the Act states that the FSOC shall designate those FMUs that it determines are, or are likely to become, systemically important. Such a designation by the FSOC makes an FMU subject to the supervisory framework set out in Title VIII of the Act.

Section 805(a)(1)(A) of the Act requires the Board to prescribe risk-management standards governing the operations related to payment, clearing, and settlement activities of designated FMUs.[5] As set out in section 805(b) of the Act, the applicable risk-management

[5] 12 U.S.C. 5464(a)(1). The Act directs the Board to "tak[e] into consideration relevant international standards and existing prudential requirements" when it promulgates these risk-management standards. *Id.* In addition, section 805(a)(2) of the Act grants the U.S. Commodity Futures Trading Commission (CFTC) and the U.S. Securities and Exchange Commission (SEC) the authority to prescribe such risk-management standards for a designated FMU that is, respectively, a derivatives clearing organization (DCO) registered under section 5b of the Commodity Exchange Act or a clearing agency registered under section 17A of the Securities Exchange Act of 1934. 12 U.S.C. 5464(a)(2).

standards must (1) promote robust risk management, (2) promote safety and soundness, (3) reduce systemic risks, and (4) support the stability of the broader financial system.[6]

A designated FMU is subject to examination by the federal agency that has primary jurisdiction over the FMU under federal banking, securities, or commodity futures laws (the "Supervisory Agency").[7] At present, the FSOC has designated eight FMUs as systemically important, and the Board is the Supervisory Agency for two of these designated FMUs – The Clearing House Payments Company, L.L.C. (on the basis of its role as operator of the Clearing House Interbank Payments System (CHIPS)) and CLS Bank International.[8] The risk-management standards in the Board's Regulation HH apply to Board-supervised designated FMUs.[9]

---

[6] Further, under section 805(c), the risk-management standards may address areas such as (1) risk-management policies and procedures, (2) margin and collateral requirements, (3) participant or counterparty default policies and procedures, (4) the ability to complete timely clearing and settlement of financial transactions, (5) capital and financial resource requirements for designated FMUs, and (6) other areas that are necessary to achieve the objectives and principles for risk-management standards. 12 U.S.C. 5464(c).

[7] The Act's definition of "Supervisory Agency" is codified at 12 U.S.C. 5462(8). Section 807 of the Act authorizes the Supervisory Agencies to examine and take enforcement actions against the Supervisory Agencies' respective designated FMUs. The Act also describes certain authorities that the Board has with respect to designated FMUs for which it is not the Supervisory Agency, such as participation in examinations and recommendations on enforcement actions. 12 U.S.C. 5466.

[8] The SEC is the Supervisory Agency for The Depository Trust Company (DTC); Fixed Income Clearing Corporation (FICC); National Securities Clearing Corporation (NSCC); and The Options Clearing Corporation (OCC). The CFTC is the Supervisory Agency for the Chicago Mercantile Exchange, Inc. (CME); and ICE Clear Credit LLC (ICC). *See* U.S. Department of the Treasury, *Financial Market Utility Designations*, https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/fsoc/designations.

[9] The risk-management standards in Regulation HH would also apply to any designated FMU for which another Federal banking agency is the Supervisory Agency. At this time, there are no such designated FMUs.

C. Regulation HH Risk-Management Standards for Designated FMUs

Section 234.3 of Regulation HH includes a set of 23 risk-management standards addressing governance, transparency, and the various risks that can arise in connection with a designated FMU's payment, clearing, and settlement activities, including legal, financial, and operational risks. These standards are based on and generally consistent with the PFMI. The Regulation HH standards generally employ a flexible, principles-based approach. In several cases, however, the Board adopted specific minimum requirements that a designated FMU must meet in order to achieve the overall objective of a particular standard.

1. Operational risk management

Section 234.3(a)(17) of Regulation HH, as amended in 2014, requires that a designated FMU manage its operational risks by establishing a robust operational risk-management framework that is approved by its board of directors.[10] Specifically, a designated FMU must (1) identify and mitigate its plausible sources of operational risk; (2) identify, monitor, and manage the operational risks it may pose to other FMUs and trade repositories; (3) ensure a high degree of security and operational reliability; (4) have adequate, scalable capacity to handle increasing stress volumes; (5) address potential and evolving vulnerabilities and threats; and (6) provide for rapid recovery and timely resumption of critical operations and fulfillment of obligations, including in the event of a wide-scale or major disruption. Section 234.3(a)(17) also contains several specific minimum requirements for business continuity planning, including a requirement for the designated FMU to have a business continuity plan that (1) incorporates the use of a secondary site at a location with a distinct risk profile from the primary site; (2) is designed to

[10] In this **Supplementary Information**, § 234.4(a)(17) will be informally referred to as the "operational risk management standard."

enable critical systems to recover and resume operations no later than two hours following disruptive events; (3) is designed to enable it to complete settlement by the end of the day of the disruption, even in case of extreme circumstances; and (4) is tested at least annually.[11]

Although the term "operational risk" is not defined in current Regulation HH, when the Board proposed amendments to § 234.3(a)(17) in 2014, it described operational risk as the risk that deficiencies in information systems, internal processes, and personnel or disruptions from external events will result in the deterioration or breakdown of services provided by an FMU.[12] Consistent with an all-hazards view of managing operational risk, the Board believes operational risk could arise internally and externally. Internal sources of operational risk include the designated FMU's people, processes, and technology.[13] External sources of operational risk are those that fall outside the direct control of a designated FMU. For example, external sources of operational risk can include the designated FMU's participants and other entities, such as other FMUs, settlement banks, liquidity providers, and service providers, which may transmit threats through their various connections to the designated FMU. External sources of operational risk also include physical events, such as pandemics, natural disasters, and other destruction of property, as well as information security threats, such as cyberattacks and technology supply chain vulnerabilities. These internal and external sources of operational risk can manifest in different scenarios (including wide-scale or major disruptions) and can result in the reduction,

---

[11] 12 CFR 234.3(a)(17)(vii).

[12] 79 FR 3666, 3683 (Jan. 22, 2014). The Board also incorporated this definition of "operational risk" into part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy) in 2014, *see* 79 FR 2838, 2845 (Jan. 16, 2014), and into its supervisory rating system for financial market infrastructure in 2016, *see* 81 FR 58932, 58936 (Aug. 26, 2016). The PSR policy is available at https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

[13] Deficiencies in assessing and managing these sources of operational risk could cause errors or delays in processing, systems outages, insufficient capacity, fraud, data loss, and data leakage.

deterioration, or breakdown of services that a designated FMU provides. A designated FMU must plan for these types of scenarios and test its systems, polices, procedures, and controls against them.

Importantly, the Board believes that effective operational risk management, in combination with sound governance arrangements and effective management of general business risk (including the risk of losses from operational events), promotes operational resilience, which refers to the ability of an FMU to: (1) maintain essential operational capabilities under adverse conditions or stress, even if in a degraded or debilitated state; and (2) recover to effective operational capability in a time frame consistent with the provision of critical services.[14]

2. Evolution in the operational risk, technology, and regulatory landscape

When the Board proposed amendments to Regulation HH's risk-management standards in 2014, the Board recognized that there was ongoing work and discussion domestically and internationally on developing operational risk-management standards and guidance and planning for business continuity with respect to cybersecurity and responses to cyberattacks.[15] For example, in 2016, the Committee on Payments and Market Infrastructures (CPMI) and Technical Committee of the International Organization of Securities Commissions (IOSCO) published *Guidance on cyber resilience for financial market infrastructures* (Cyber Guidance), which supplements the PFMI and provides guidance on cyber resilience, including in the context of

[14] *See* § 234.3(a)(2) and (a)(15).

[15] 79 FR at 3683.

governance, the comprehensive management of risks, and operational risk management.[16] The Cyber Guidance has informed the Federal Reserve's supervision of designated FMUs.[17]

More recently, new challenges to operational risk management have emerged, including a global pandemic and severe weather events. In addition, certain types of cyberattacks that were once thought to be extreme or "tail-risk" events, like attacks on the supply chain and ransomware attacks, have become more prevalent. Technology solutions for the mitigation and management of various operational risks have also advanced since 2014, including the development of new technologies that have the potential to improve the resilience of designated FMUs. Finally, the legal, regulatory, and supervisory landscape in which designated FMUs operate has evolved to reflect these changes in the broader operational risk environment. For example, in July 2021, the Board, the Office of the Comptroller of the Currency (OCC), and the Federal Deposit Insurance Corporation (FDIC) proposed guidance for banking organizations on managing risks associated with third-party relationships.[18] In November 2021, the Board, OCC, and FDIC adopted requirements on computer-security incident notifications for banking organizations and bank service providers (interagency notification rule).[19] The evolution in the operational risk, technology, and regulatory landscape motivated the Board to conduct a full review of

---

[16] CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016), https://www.bis.org/cpmi/publ/d146.htm.

[17] For example, when the Board finalized its ORSOM rating system for designated FMUs in 2016, it noted that the then-forthcoming Cyber Guidance would guide the Board's assessment of a designated FMU with respect to operational risk and cybersecurity policies and procedures. 81 FR at 58934 .

[18] 86 FR 38182 (July 19, 2021). The Board, OCC, and FDIC issued final third-party risk management guidance for banking organizations in June 2023. 88 FR 37920 (June 9, 2023).

[19] 86 FR 66424 (Nov. 23, 2021). Congress also recently enacted the Cyber Incident Reporting for Critical Infrastructure Act of 2022, which requires covered entities to report significant cyber incidents to the Cybersecurity and Infrastructure Agency ("CISA"). *See* Pub. L. 117-103, Div. Y (codified at 6 U.S.C. 681-681g).

§ 234.3(a)(17) to determine whether updates were necessary. Following this review, the Board believes that the outcomes required by the current operational risk management standard are generally still relevant and comprehensive. However, the Board has identified several areas where it believes updates to the rule are necessary.

D. Overview of the Proposal

The Board proposed to amend the operational risk management standard to reflect changes in the operational risk and threat landscape, as well as to reflect developments in designated FMUs' operations and technology usage since the Board last amended Regulation HH in 2014. The proposed amendments focused on four areas: (1) review and testing, (2) incident management and notification, (3) business continuity management and planning, and (4) third-party risk management. The Board also proposed several technical or clarifying revisions throughout §§ 234.2 and 234.3(a).[20]

III. Summary of Public Comments and Analysis

The Board received six public comment letters. Two letters were from entities that operate designated FMUs, one letter was from a non-profit organization, and three letters were from individuals. The Board considered each of these comments as well as subsequent staff analysis in developing the final rule. The Board is adopting the proposed rule text with modifications to certain sections, as discussed below.

[20] In addition to the technical changes described below in section III.G, the Board proposed a technical change to the title of § 234.3. Currently, the section is erroneously titled "Standards for payment systems," which is the legacy title from the initial Regulation HH risk-management standards published in 2012. The Board proposed to replace "payment systems" with "designated financial market utilities."

A. Overall Response and Approach

Commenters were generally supportive of the proposed amendments. Of the three substantive comments received, one commenter expressed support for the amendments as proposed. Two commenters, while expressing support for the overall proposal, raised concerns that aspects of the proposal were broader than necessary. These commenters suggested additional clarifications to and refinements in the scope of the proposed amendments. Both of these commenters raised concerns that amendments to Regulation HH should permit a designated FMU to apply a risk-based and proportionate approach to operational risk management. This comment was made both generally and with respect to specific aspects of the review and testing, business continuity management and planning, and third-party risk management sections of the proposed amendments. The Board generally understands a "risk-based and proportionate approach" as an approach whereby entities identify, assess, and understand the risks to which they are exposed and take measures commensurate with those risks.[21]

The final rule does not expressly specify that designated FMUs may use a risk-based and proportionate approach to comply with the amended operational risk management standard. The Board believes that it is unnecessary to do so. Designated FMUs currently use risk-based and proportionate approaches to manage operational risk, as the Board generally has implemented principles-based requirements in Regulation HH. The proposed amendments were not intended to affect designated FMUs' ability to continue to use risk-based and proportionate approaches where appropriate. Furthermore, other parts of Regulation HH's risk-management standards, such as the framework for the comprehensive management of risks found in § 234.3(a)(3), do not

[21] *See* Cyber Guidance, *supra* note 16, at 26.

expressly specify a risk-based and proportionate approach. Thus, adding such language to the operational risk management standard could result in a difference in drafting not driven by a difference in intended meaning.

The Board has, however, amended certain aspects of the proposal to incorporate several specific concerns raised by the commenters. These concerns and the Board's response are described in the sections that follow.

B. Compliance Date

In the NPRM, the Board proposed an effective and compliance date of 60 days from the date the final rule was published in the *Federal Register*. Two commenters expressed the need for additional time to comply with the final rule and requested 180 days after publication to comply. Specifically, these commenters requested more time to enable designated FMUs to assess their current procedures and practices against the amendments and to implement any necessary changes. They also noted that the proposed third-party risk management requirements might necessitate changes to designated FMUs' contracts with third parties, which might take longer than 60 days. One commenter explained that it would take longer than 60 days to implement the incident notification requirement of the Board's proposed incident management framework. A third commenter considered the Board's amendment of the operational risk management standard overdue and viewed incident management and notification as the most important part of the proposal.

The Board is adopting the final rule with an effective date of **[INSERT DATE THAT IS 30 DAYS FROM PUBLICATION IN THE FEDERAL REGISTER]**. Designated FMUs are expected to comply with the requirements of the final rule no later than [INSERT DATE THAT IS 180 DAYS AFTER PUBLICATION], with the exception of the requirement to establish a

documented framework for incident management, set forth in in § 234.3(a)(17)(vi). Designated FMUs are expected to comply with § 234.3(a)(17)(vi) no later than [INSERT DATE THAT IS 90 DAYS AFTER PUBLICATION]. Designated FMUs are encouraged, however, to comply with the provisions as soon as possible.

After consideration of the public comments as well as internal analysis, the Board is providing additional time to allow sufficient time for designated FMUs to review their existing policies, procedures, practices, and contracts against the requirements of the final rule and to minimize burden on designated FMUs and the markets they serve. However, the Board adopted an earlier compliance date for the requirement to establish a documented framework for incident management, set forth in § 234.3(a)(17)(vi). The Board believes that designated FMUs can leverage existing practices for incident management and notification and that an earlier compliance date balances the need for prompt conformance with § 234.3(a)(17)(vi), which the Board considers of critical importance to both the Board and designated FMUs' participants and other stakeholders, with the overall burden on designated FMUs.

C. Review and Testing

Section 234.3(a)(17)(i) of Regulation HH requires designated FMUs to identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls that are reviewed, audited, and tested periodically and after major changes. This general review and testing requirement applies broadly to the systems, policies, procedures, and controls that the designated FMU develops to mitigate sources of operational risk. The Board proposed to amend § 234.3(a)(17)(i) to provide more specificity regarding its expectations around testing, review, and remediation. Just as the current general review and testing requirement in § 234.3(a)(17)(i)

applies broadly to a designated FMU's systems, policies, procedures, and controls, the proposed amendments would also apply broadly to the systems, policies, procedures, and controls developed to mitigate the impact of the designated FMU's sources of operational risk.

Specifically, proposed § 234.3(a)(17)(i)(A) and (B) set forth the Board's expectations regarding review and testing. In § 234.3(a)(17)(i)(A)(1), the Board proposed to require a designated FMU to conduct tests of its systems, policies, procedures, and controls in accordance with a documented testing framework.[22] The Board further proposed in § 234.3(a)(17)(i)(A)(2) to require that a designated FMU's testing assess whether its systems, policies, procedures, or controls function as intended.[23]

In § 234.3(a)(17)(i)(B), the Board proposed to require a designated FMU to conduct a review of the design, implementation, and testing of systems, policies, procedures, and controls after the designated FMU experienced any material operational incidents (which are discussed in section III.C.1 below). The Board also proposed in § 234.3(a)(17)(i)(B) to require a designated

[22] The Board explained in the NPRM that the testing framework should account for any interdependencies between and among the systems, policies, procedures, and controls that are being tested. The Board further explained that a designated FMU should take a comprehensive and risk-based approach to its operational risk management testing program, rather than focusing only on testing individual (or groups of) systems, policies, procedures, or controls (or components therein). A designated FMU could describe its testing framework in either a single document or in multiple documents, as appropriate, and could leverage relevant industry standards as it develops its testing framework. For example, a designated FMU could leverage standards developed by the National Institute of Standards and Technology (NIST), the Federal Financial Institutions Examination Council (FFIEC), the Financial Services Sector Coordinating Council (FSSCC), and the International Organization for Standardization (ISO).

[23] Such tests could include capacity stress tests, crisis management tabletop exercises, after-action reviews of incidents, business continuity tests both internally and with participants, vulnerability assessments, cyber scenario-based testing, penetration tests, and red team tests.

FMU to review the design, implementation, and testing of systems, policies, procedures, and controls after significant changes to the environment in which it operates.[24]

Finally, the Board proposed in § 234.3(a)(17)(i)(C) to require a designated FMU to remediate, as soon as possible and following established governance processes, any deficiencies identified during tests and reviews.

1. Review and testing—Section 234.3(a)(17)(i)(A)-(B)

a) Summary of Comments

One commenter welcomed the additional clarity provided by the proposed amendments to § 234.3(a)(17)(i) generally, and another commenter appreciated the proposal's testing and review expectations. Two commenters suggested that all of § 234.3(a)(17)(i), including subsections (A), (B), and (C), be amended to expressly contemplate the designated FMU taking a risk-based approach to testing, review, and remediation activities.

Commenters did not suggest other revisions to proposed § 234.3(a)(17)(i)(A). With respect to the proposed review requirements set out in § 234.3(a)(17)(i)(B), two commenters raised a concern that the proposed language could be interpreted to require a designated FMU to review *all* of its systems, policies, procedures, and controls after a material operational incident or significant change to the environment in which the designated FMU operates. These commenters suggested clarifying that § 234.3(a)(17)(i)(B) require review of only the *relevant*

[24] The Board also proposed a technical amendment to the requirement for the designated FMU to review its recovery and orderly wind-down plan under § 234.3(a)(3)(iii)(G) from "following" to "after" changes to the designated FMU's systems and environment. This conforms with the review requirement under proposed § 234.3(a)(17)(i)(B). The Board also proposed a technical amendment to the requirement for the designated FMU to update its public disclosure under § 234.3(a)(23)(v) from "following" to "to reflect" changes to its systems and environment. The Board did not receive any comments on these technical amendments and is adopting them as proposed.

systems, policies, procedures, and controls affected by material operational incidents or significant changes to the environment.

One commenter further suggested that, in the case of significant changes to the environment, § 234.3(a)(17)(i)(B) require a review only when the change is reasonably likely to create operational risk. The commenter noted such an approach would avoid reviews when there are changes to the environment that do not reasonably create operational risk.

b) Final Rule

The Board is adopting proposed § 234.3(a)(17)(i)(A) and (B) with certain revisions based on internal analysis and public comments.

Consistent with the preamble to the proposed rule, the Board has clarified in § 234.3(a)(17)(i)(A)(1) that a designated FMU's documented testing framework must address *at a minimum* scope, frequency, participation, interdependencies, and reporting. A designated FMU may also choose to add additional pieces to their documented testing frameworks based on their own internal analysis. This could include documented governance processes around review and testing. Importantly, as described further below, a designated FMU would need to remediate deficiencies identified during testing, following established governance processes.

The Board has adopted two amendments to proposed § 234.3(a)(17)(i)(B). First, the Board has modified the rule text in § 234.3(a)(17)(i)(B) to reflect that a designated FMU's review of design, implementation, and testing after material operational incidents or after changes to the environment in which the designated FMU operates applies only to *affected and similar* systems, policies, procedures, and controls. The Board agrees with commenters that a

designated FMU need not review irrelevant systems, policies, procedures, and controls.[25] The Board would consider relevant systems, policies, procedures, and controls to include those affected directly by a material operational incident or significant change to the environment. In addition, the Board would consider relevant systems, policies, procedures, and controls to include those that have not been directly affected but that share important features with (*i.e.*, are similar to) affected systems, policies, procedures, and controls. For example, a similar system could be one that is susceptible to the same type of vulnerability that has caused a material operational incident in a different system, but which was not actually affected in a particular instance.

Second, consistent with statements in the preamble to the NPRM and in response to comments, the Board has clarified that § 234.3(a)(17)(i)(B) requires designated FMUs to conduct reviews when a change to the environment in which the designated FMU operates could significantly affect the plausible sources or mitigants of operational risk.[26] Designated FMUs should exercise care to ensure that they effectively identify changes to the environment that have an operational risk component, but the review requirement would not be triggered by a change that does not relate to operational risk.

For the reasons described in section III.A, *supra*, the Board has not expressly referred to a risk-based and proportionate approach in the final rule. With respect to testing, § 234.3(a)(17)(i)(A)(1) requires a designated FMU's documented testing framework to address,

[25] *See* 87 FR 60314, 60317 (Oct. 5, 2022) (proposing that a designated FMU conduct a review of the design, implementation, and testing of relevant systems, policies, procedures, and controls after the designated FMU experiences any material operational incidents).

[26] *See id.* (explaining that the operational risk environment, including sources of risk and the nature or types of threats, can change unexpectedly and quickly and that the proposal would ensure that designated FMUs review and make timely changes to their systems, policies, procedures, and controls following such changes).

at a minimum, scope, frequency, participation, interdependencies, and reporting—all of which could be calibrated based on a designated FMU's identification, assessment, and prioritization of risks.[27] With respect to review, the Board believes the requirement to conduct reviews after certain events is consistent with a risk-based approach. Moreover, the two clarifications the Board has made to § 234.3(a)(17)(i)(B) focus the requirements of that paragraph on the review triggers that the Board considers most important for a designated FMU's management of operational risk.

2. Remediation of identified deficiencies—Section 234.3(a)(17)(i)(C)

a) Summary of Comments

Similar to the comments on the testing and review requirements, two commenters suggested that the rule text clarify that a designated FMU may take a risk-based approach to the remediation process. One commenter specifically recommended that the rule allow a designated FMU to remediate or mitigate an identified deficiency in a manner that is consistent with the designated FMU's risk appetite. As part of a risk-based approach, one commenter suggested that a designated FMU should be able to accept the risks associated with certain deficiencies so long as the risks are within the designated FMU's risk appetite.

One commenter noted that, while proposed § 234.3(a)(17)(i)(C) stated that a designated FMU's remediation of deficiencies in systems, policies, procedures, or controls should follow established governance processes, it was unclear if the requirement to follow governance processes referred solely to the need to validate remediation steps or if it was intended to be broader. The commenter suggested that governance processes for managing and overseeing

[27] The Board expects that, in developing its documented testing framework, a designated FMU would be guided by the documented risk-management framework established by the board of directors, which must include, among other things, the designated FMU's risk-tolerance policy. 12 CFR 234.3(a)(2)(iv)(F).

remediation should include processes for decision making on prioritization of remediation approaches in addition to validation. One commenter noted that the proposed rule did not address expectations regarding validation of remediation steps. The commenter suggested that validation should be risk-based and proportionate to the deficiency that is being remediated.

b) Final Rule

The Board is adopting § 234.3(a)(17)(i)(C) with one modification in response to concerns raised by commenters.[28] In order to address concerns that the proposal would have required a designated FMU to approach all deficiencies in the same manner, the Board has removed the word "any" from proposed § 234.3(a)(17)(i)(C).[29] In addition, the Board expects that a designated FMU, in establishing the governance processes contemplated by § 234.3(a)(17)(i)(C), would take into account the designated FMU's risk-tolerance policy.[30] In that regard, the Board notes that remediation could include both actions to eliminate a deficiency or vulnerability or to reduce the risk associated with a deficiency or vulnerability to an acceptable level.[31] For

---

[28] For the reasons described in section III.A, *supra*, the Board has not expressly referred to a risk-based and proportionate approach in the final rule.

[29] As noted above, proposed § 234.3(a)(17)(i)(C) would have required a designated FMU to remediate, as soon as possible and following established governance processes, *any* deficiencies identified during tests and reviews.

[30] A designated FMU must have governance arrangements that, among other things, are designed to ensure that the board of directors establishes a clear, documented risk-management framework that includes the designated FMU's risk-tolerance policy, assigns responsibilities and accountability for risk decisions, and addresses decision making in crises and emergencies. 12 C.F.R. 234.3(a)(2)(iv)(F).

[31] The Board understands that the terms "remediation" and "mitigation" are sometimes used in different ways in the information technology and security field. The Board's use of "remediation" and "mitigation" is consistent with NIST's definitions of the terms. NIST defines "remediation" as "the act of mitigating a vulnerability or a threat," and "mitigation" as "a decision, action, or practice intended to reduce the level of risk associated with one or more threat events, threat scenarios, or vulnerabilities." These definitions can be found at https://csrc.nist.gov/glossary/term/remediation and https://csrc.nist.gov/glossary/term/mitigation, respectively.

example, if a designated FMU were to identify a deficiency in a system that was slated for replacement in the near future, the designated FMU could consider steps to reduce the risk of that deficiency pending the implementation of the new system in lieu of working to eliminate the deficiency in the old system. When consistent with a designated FMU's risk tolerance and otherwise consistent with a robust operational risk framework, a designated FMU could determine and document its decision to accept the risk of a deficiency.

The Board expects that a designated FMU will conduct an internal risk analysis of all deficiencies identified in review and testing, as required in § 234.3(a)(17)(i)(A) and (B), and use established governance processes to determine how to address and prioritize identified deficiencies in order to reduce the level of risk posed by those deficiencies.[32] The decisions a designated FMU makes may depend upon the facts and circumstances.[33]

Finally, commenters noted that proposed § 234.3(a)(17)(i)(C) did not specifically address validation but that the NPRM stated that it would be imperative for a designated FMU to perform subsequent validation to assess whether the remediation measures have addressed deficiencies without introducing vulnerabilities. The Board continues to believe that designated FMUs should assess the effectiveness and broader impact of any changes they make to remediate a deficiency.[34] The Board acknowledges that the validation performed may depend on the nature of both the deficiency and any changes made to remediate the deficiency. As with remediation,

[32] As noted above, a designated FMU's documented testing framework could address governance processes for remediation.

[33] A designated FMU should consult widely used and relevant industry standards to inform its understanding of how it should remediate deficiencies. These industry standards, such as those published by NIST, FFIEC, FSSCC, and ISO, are updated regularly and typically offer current and specific information on operational risk management practices.

[34] In the event a designated FMU accepts the risk of a deficiency, there may be no change to validate.

the Board believes that a designated FMU, in its governance processes, could address validation in a risk-based manner.

D. Incident Management and Notification

The Board proposed in § 234.3(a)(17)(vi) to require a designated FMU to establish a documented framework for incident management that provides for the prompt detection, analysis, and escalation of an incident; appropriate procedures for addressing an incident; and incorporation of lessons learned following an incident.[35]

Specifically, in § 234.3(a)(17)(vi) the Board proposed to require that a designated FMU's incident management framework include a plan for notification and communication of material operational incidents. This plan, among other things, would need to identify the entities that would be notified of operational incidents, including non-participants that could be affected by material operational incidents at the designated FMU. Relevant entities may also include appropriate industry information-sharing fora, such as groups that are designed to share information about cyber threats or support cyber risk management.

In § 234.3(a)(17)(vi)(A), the Board proposed to require a designated FMU to notify the Board immediately when it activated its business continuity plan or had a reasonable basis to conclude that (1) there was an actual or likely disruption, or material degradation, to any of its critical operations or services,[36] or to its ability to fulfill its obligations on time; or (2) there was unauthorized entry, or the potential for unauthorized entry, into the designated FMU's computer,

---

[35] These broad categories in incident management are generally consistent with those identified in the NIST computer-security incident handling guide. *See* NIST, *Computer Security Incident Handling Guide* (Special Publication 800-61, rev. 2), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf.

[36] Critical operations and critical services are discussed below in section III.G.2.

network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services.

In § 234.3(a)(17)(vi)(B), the Board proposed to require a designated FMU to establish criteria and processes, including the appropriate methods of communication, to provide for timely communication and responsible disclosure of material operational incidents to its participants or other relevant entities that have been identified in its notification and communication plan. As proposed, this incident notification requirement would arise in two circumstances. First, under proposed § 234.3(a)(17)(vi)(B)(1), a designated FMU would need to notify affected participants immediately in the event of actual disruptions or material degradation to its critical operations or services or to its ability to fulfill its obligations on time. Second, under proposed § 234.3(a)(17)(vi)(B)(2), a designated FMU would need to notify all participants and other relevant entities in a timely and responsible manner of all other material operational incidents that require immediate notification to the Board.[37]

1. Documented incident management framework—Section 234.3(a)(17)(vi)

a) Summary of Comments

One commenter broadly supported the proposal and viewed incident management and notification as the most important part of the Board's proposed amendments to Regulation HH. Two commenters did not object in concept to the requirement for a documented framework for incident management but expressed concerns with specific aspects of the proposed requirement to have a plan for notification and communication of material operational incidents. These concerns are discussed in sections III.D.2 and III.D.3, *infra*.

[37] As noted in the NPRM, a designated FMU would need to identify non-participant relevant entities in its plan for notification and communication of material operational incidents.

b) Final Rule

The Board is adopting the introductory portion of § 234.3(a)(17)(vi) as proposed and, as discussed below, has adopted subsections § 234.3(a)(17)(vi)(A) and (B) with certain modifications. In line with the all-hazards approach to operational risk management in this standard, the Board reiterates its belief that it is important for a designated FMU to be prepared to detect, address, and learn from any type of operational incident, regardless of the scenario or source of risk and the level of severity. Different types of incidents may require different levels of escalation internally or externally, and may require different strategies for containment or eradication. For example, given the increasing prevalence of cyberattacks in the financial sector, a designated FMU should plan for an incident where a participant (or another type of connected entity), rather than the designated FMU itself, is experiencing a cyberattack. In this scenario, a designated FMU should be operationally prepared to take, and should have a legal basis to take, appropriate steps to mitigate the risk of contagion to itself or other participants, including, but not limited to, restricting or limiting a participant's access to the designated FMU or a particular functionality or disconnecting the participant from the FMU if necessary. Relatedly and as further discussed in section III.E.3, a designated FMU should also have processes and procedures to determine whether and when it would be appropriate to reestablish availability to such a participant.

2. Incident notification to the Board—Section 234.3(a)(17)(vi)(A)

a) Summary of Comments

Two commenters expressed concerns regarding the circumstances that would trigger a notice requirement to the Board. One commenter noted that proposed § 234.3(a)(17)(vi)(A) would require a designated FMU to notify the Board any time the designated FMU activated its business continuity plan. This commenter highlighted that activation of the business continuity

plan may not involve an actual disruption to the designated FMU's critical operations or services and that the proposal could result in unnecessary notifications. Two commenters indicated concern with the words "likely" in proposed § 234.3(a)(17)(vi)(A)(1) and "potential" in proposed § 234.3(a)(17)(vi)(A)(2). The concerns raised include providing notifications where it was unnecessary, the potential for false alarms or misimpressions regarding a designated FMU's reliability, and desensitization of supervisors and participants due to excessive notification regarding insignificant events, with one commenter suggesting notices be limited to actual incidents. One commenter also noted that the "likely" and "potential" standards were different from other incident notification requirements such as under the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) and suggested harmonizing the proposed notification requirements with other laws and regulations.

These commenters suggested a number of specific revisions to the proposal. One suggested limiting notification to the Board to actual disruptions or material degradations. Another suggested limiting notifications of an unauthorized entry, or the potential for unauthorized entry, to situations which could result in a serious detriment to participants or other relevant entities, and more generally suggested granting more discretion for a designated FMU to determine appropriate circumstances for notice based on the probability and severity of an event.

One commenter supported the requirement to provide "immediate" notification to the Board and affected parties. Two commenters requested clarification of the term "immediately" as used regarding notification of material operational incidents in proposed § 234.3(a)(17)(vi)(A) and § 234.3(a)(17)(vi)(B)(1). These commenters requested that the explanation provided in the NPRM, which distinguished "immediately" from "instantaneous," be directly incorporated into

the text of Regulation HH. One commenter suggested that such a revision would provide greater clarity to participants and other relevant entities.

Finally, two commenters responded to a question in the NPRM regarding the process by which a designated FMU should provide notice to the Board. These commenters suggested that notices be provided to the team responsible for ongoing supervision of the designated FMU. One of the commenters noted that a designated FMU's supervisory team would likely continue to expect notice regardless of whether a designated FMU was required to notify a central point of contact. One of the commenters also suggested that the Board specify contacts and provide a method for delivering notices outside of business hours.

b) Final Rule

The Board is adopting § 234.3(a)(17)(vi)(A) as proposed, with two revisions that respond to comments received. First, as proposed, § 234.3(a)(17)(vi)(A)(2) would have required notice to the Board of an unauthorized entry, or a *potential* for unauthorized entry, into a designated FMU's computer, network, electronic, technical, automated, or other systems that affect or have the potential to affect its critical operations or services. In light of concerns regarding unnecessary notices, the Board believes it is appropriate to clarify what constitutes the "potential" for unauthorized entry. The Board has amended § 234.3(a)(17)(vi)(A)(2) to refer instead to an unauthorized entry *or a vulnerability that could allow unauthorized entry*. The Board believes that it is important to receive notice from a designated FMU if the designated FMU has a reasonable basis to conclude that there exists a vulnerability (such as a zero-day vulnerability) that may be, but has not yet been, exploited.[38]

[38] "Zero-day" vulnerabilities are those for which patches are not yet available. *See, e.g.*, Board of Governors of the Federal Reserve System, Cybersecurity and Financial System Resilience

Second, the Board has clarified that a designated FMU must notify the Board of incidents "in accordance with the process established by the Board." The Board will provide actual notice of this process to affected designated FMUs.

Other than with respect to these revisions, the Board has adopted § 234.3(a)(17)(vi)(A) as proposed. Given the large volume and value of payment, clearing, and settlement activity processed by designated FMUs and their interconnectedness with financial institutions and markets, material operational issues occurring at designated FMUs could have financial stability implications. Therefore, the Board continues to believe that it is critical for the Board to be notified immediately of these types of issues.[39] The Board notes that "immediately" as used in § 234.3(a)(17)(vi)(A) is meant to convey the urgency in notifying the Board of these material operational incidents. "Immediate" does not mean "instantaneous," and as such the Board does not believe clarification expressly stating this is necessary. The Board would expect to be notified of an operational incident once the designated FMU activates its business continuity plan or has a reasonable basis to conclude that an incident meets any of the criteria in § 234.3(a)(17)(vi)(A), even if the designated FMU does not yet have detailed information on the root cause or measures for containment or remediation. In these cases, the Board would expect to receive any available information that the designated FMU has at the time of notification.

Report, at 23 (Aug. 2023), *available at* https://www.federalreserve.gov/publications/files/cybersecurity-report-202308.pdf.

[39] The Board recognizes that, "immediately" poses a heightened requirement for notification by designated FMUs relative to banking organizations subject to the interagency rule. This heightened requirement is consistent with the systemic importance of designated FMUs and in line with expectations for designated FMUs for which the SEC is the Supervisory Agency. SEC Regulation SCI provides for immediate notification to the SEC upon any "responsible SCI personnel" having a reasonable basis to conclude that an "SCI event" has occurred. *See* 17 CFR 242.1002(b)(1).

Except as described above, the Board continues to believe that notification is appropriate when a designated FMU has a reasonable basis to conclude that there is (1) an actual *or likely* disruption or material degradation to any critical operations or services, or to its ability to fulfill its obligations on time or (2) an unauthorized entry, or a vulnerability that could allow unauthorized entry, into the designated FMU's computer, network, electronic, technical, automated, or similar systems that affects *or has the potential to affect* its critical operations or services. The Board appreciates commenters' interest in harmonizing notice requirements. However, the Board notes that the interagency notification rule applies to banking organizations and bank service providers broadly, whereas Regulation HH applies to FMUs that have been designated as systemically important by the FSOC. The Board acknowledges that CIRCIA provides for after-the-fact reporting of incidents. The Board believes receiving notices of actual and likely incidents as soon as the designated FMU is aware of them is appropriate given the Board's supervisory role and the systemic importance of designated FMUs.

For the same reasons, the Board does not believe it is appropriate to limit notice to the Board with respect to unauthorized entries, or vulnerabilities that could allow unauthorized entry, to situations that could result in a serious detriment to participants or other relevant entities or to afford designated FMUs discretion to determine appropriate circumstances for notice based on the probability and severity of an event.

Similarly, the Board understands that activation of a business continuity plan does not mean an actual incident must have occurred. Activation does mean, however, that the probability of an event occurring that could adversely impact the designated FMU's continued operations was high enough to meet the threshold for the designated FMU to trigger its business

continuity plan.[40] Accordingly, the Board believes a designated FMU should notify the Board when it activates its business continuity plan.

3. Incident notification to participants and other relevant entities—Section 234.3(a)(17)(vi)(B)

a) Summary of Comments

As noted above with respect to notices required to be made to the Board, one commenter noted it was judicious and sensible to require designated FMUs to immediately notify affected participants of material operational incidents. Two commenters requested clarification of the term "immediately" as used regarding notification of material operational incidents in proposed § 234.3(a)(17)(vi)(B)(1). One commenter suggested revising the proposed notification requirement in § 234.3(a)(17)(vi)(B)(1), for the same reasons outlined in their comments for proposed § 234.3(a)(17)(vi)(A)(1), by limiting it to actual disruptions or material degradations to a designated FMU's critical operations or services, or to the designated FMU's ability to fulfill its settlement obligations on time, that *could result in a serious detriment to participants or other relevant entities*. The commenter suggested that the addition of the italicized language would permit the designated FMU to comply with the regulatory requirements while liaising with supervisors to ensure the notification provided to participants and other entities meets supervisory expectations.

One commenter expressed concern that the requirements under proposed § 234.3(a)(17)(vi)(B)(2) could result in false alarms to third parties, give an impression of

[40] For example, if a designated FMU activates its business continuity plan in anticipation of an extreme weather event, the Board would expect to be notified. The Board should be made aware if the designated FMU anticipates non-business-as-usual actions or operations.

unreliability, or desensitize parties to notifications. The commenter proposed that § 234.3(a)(17)(vi)(B)(2) be amended to only require notification for actual incidents or actual unauthorized entries.

b) Final Rule

The Board is adopting proposed § 234.3(a)(17)(vi)(B) with certain revisions to clarify the circumstances in which the Board expects a designated FMU to provide notice of material operational incidents to participants (including unaffected participants) and other relevant entities, consistent with the concept of "responsible disclosure," and to respond to commenters' concerns that disclosure under proposed § 234.3(a)(17)(vi)(B) could result in false alarms to third parties, give an impression of unreliability, or desensitize parties to notifications.

With respect to § 234.3(a)(17)(vi)(B)(2), the Board believes there are scenarios where all participants and identified relevant entities should be informed of likely disruptions or vulnerabilities that could allow for unauthorized entry into the designated FMU's computer, network, electronic, technical, automated, or similar systems, even where no incident or unauthorized access happens. The Board recognizes, though, that notification of certain likely incidents or vulnerabilities may not be required. Under the final rule, a designated FMU should establish criteria and processes for timely communication and responsible disclosure that guide whether and when it is appropriate to notify in a responsible manner entities of a particular incident. For example, consistent with the concept of responsible disclosure, the Board recognizes that there might be risks to providing early disclosures under § 234.3(a)(17)(vi)(B)(2) to a broad audience regarding certain types of material operational issues. The Board would expect a designated FMU, in practicing responsible disclosure, to account for both the benefit of the information to be provided in a notification and the potential risk of disclosing that information. For example, if a designated FMU identifies a cyber vulnerability, the designated

FMU might weigh the risk of disclosure as sufficiently great to delay notification under § 234.3(a)(17)(vi)(B)(2) or tailor the information provided under § 234.3(a)(17)(vi)(B)(1) or (2) to avoid exposing the designated FMU to a cyberattack. The Board also recognizes the risks of over-notification and of reporting false alarms to a broad audience. Notice under § 234.3(a)(17)(vi)(B)(2) of incidents that are resolved without disruption may provide little benefit to participants or identified relevant entities. In addition, a designated FMU that provides notification to the Board under the "reasonable basis" standard set forth in § 234.3(a)(17)(vi)(A) may subsequently determine there to have been a false alarm. Under such circumstances, a designated FMU could determine that broad disclosure under § 234.3(a)(17)(vi)(B)(2) is not appropriate. Consistent with concerns raised by one commenter, a designated FMU could incorporate consultation with its supervisors in the development of criteria and processes with respect to novel or complex incidents.

When designing its communication plan, the Board would expect a designated FMU to consider the timing, content, recipients, and method of notification for a range of potential material operational incidents. In determining the scope of disclosure for a particular incident, the Board would expect a designated FMU to consider factors such as the risk-mitigation benefits arising from early warning to the financial system, the safety and soundness of the designated FMU, and any financial stability implications of disclosure.

4. Examples of material operational incidents

The following is a non-exhaustive list of operational incidents that the Board would consider to be material for purposes of the final rule.[41] The Board would expect examples 1–3 to

[41] The NPRM included a list of examples. The Board did not receive any specific comments on the examples. The Board has expanded on that list to provide further clarity.

trigger immediate notifications to the Board and to the designated FMU's affected participants (and notification in a timely manner to unaffected participants and other relevant entities identified in the designated FMU's plan for notification and communication of material operational incidents, as applicable).

1) A failed system upgrade or change results in widespread user outages for participants and designated FMU employees.
2) Large-scale distributed denial of service attacks that prevent the designated FMU from receiving its participants' payment instructions.
3) A severe weather event or other natural disaster that causes significant damage to a designated FMU's production site and disrupts core payment, clearing, or settlement processes, necessitating failover to another site during the business day.

The Board would expect examples 4–7 to trigger immediate notification to the Board, but a designated FMU would determine when and whether to notify participants and other relevant entities based on the criteria in its notification and communication plan.

4) A severe weather event or other natural disaster that causes significant damage to a designated FMU's production site and necessitates failover to another site during the business day, but the designated FMU's core payment, clearing, or settlement processes remain available to participants.
5) Malware on a designated FMU's network that poses an imminent threat to its critical operations or services (such as its core payment, clearing, or settlement processes, or collateral management processes), or that may require the designated FMU to disengage any compromised products or information systems

that support the designated FMU's critical operations and services from internet-based network connections.

6) A ransom malware attack that encrypts a critical system or backup data.

7) A zero-day vulnerability on software that the designated FMU uses and has determined, if exploited, could lead to a disruption to or material degradation of its critical operations or services.

E. Business Continuity Management and Planning

Section 234.3(a)(17)(vi) of the current rule (under the proposal, renumbered as § 234.3(a)(17)(vii)) requires that a designated FMU have business continuity management that provides for rapid recovery and timely resumption of its critical operations and fulfillment of its obligations, including in the event of a wide-scale or major disruption.[42]

Section 234.3(a)(17)(vii) of the current rule (under the proposal, renumbered § 234.3(a)(17)(viii)) elaborates on certain requirements for a designated FMU's business continuity plan. The Board proposed to amend current § 234.3(a)(17)(vii) to provide further detail in Regulation HH related to business continuity management and planning in order to promote robust risk management, reduce systemic risks, increase safety and soundness, and support the stability of the broader financial system.

Specifically, the Board proposed to amend current § 234.3(a)(17)(vii)(A) to update terminology related to required backup sites. The Board proposed to replace the references to a "secondary site" and "primary site" with a general reference to "two sites providing for sufficient redundancy supporting critical operations and services" that are located at a sufficient

[42] The Board proposed a technical revision to that section, as described in section III.G.2, *infra*.

geographical distance from "each other" to have a distinct risk profile (collectively, "two sites with distinct risk profiles").

The Board did not propose substantive amendments to the requirements under current §§ 234.3(a)(17)(vii)(B) and (C) (renumbered as §§ 234.3(a)(17)(viii)(B) and (C)), which require a designated FMU's business continuity plan to be designed to enable recovery and resumption no later than two hours following disruptive events and completion of settlement by the end of the day of the disruption, even in case of extreme circumstances. The Board proposed a technical amendment to § 234.3(a)(17)(vii)(B) to clarify that the two-hour recovery time objective applies to critical operations and services.[43]

In § 234.3(a)(17)(viii)(D), the Board proposed to require that a designated FMU's business continuity plan set out criteria and processes that address the reconnection of a designated FMU to its participants and other entities following a disruption to the designated FMU's critical operations or services.

The Board proposed to separate current § 234.3(a)(17)(vii)(D) of Regulation HH, which requires the business continuity plan to be "tested at least annually," into two requirements (renumbered as § 234.3(a)(17)(viii)(E) and (F)). In § 234.3(a)(17)(viii)(E), the Board proposed to maintain the requirement for at least annual testing and clarify that this requirement covers the designated FMU's business continuity arrangements, including the people, processes, and technologies of the two sites with distinct risk profiles.[44] The Board proposed to require a designated FMU's testing to demonstrate that the designated FMU is able to run live production at the two sites with distinct risk profiles; that its solutions for data recovery and data

[43] *See* section III.G.2, *infra*.
[44] These tests would be subject to the general testing requirements described in section III.C.1 above.

reconciliation enable it to meet its objectives to recover and resume operations two hours following a disruption and enable settlement by the end of the day of the disruption even in case of extreme circumstances, including if there is data loss or corruption; and that it has geographically dispersed staff who can effectively run the operations and manage the business of the designated FMU.

In § 234.3(a)(17)(viii)(F), the Board proposed to require a designated FMU to review its business continuity plans, pursuant to the general review requirements described in section III.C.1 above, at least annually, to: (1) incorporate lessons learned from actual and averted disruptions, and (2) update the scenarios considered and assumptions built into the plan in order to ensure responsiveness to the evolving risk environment and incorporate new and evolving sources of operational risk (*e.g.*, extreme cyber events).

1. Two sites providing for sufficient redundancy—Section 234.3(a)(17)(viii)(A)

a) Summary of Comments

The Board received no comments on proposed § 234.3(a)(17)(viii)(A).

b) Final Rule

The Board is adopting § 234.3(a)(17)(viii)(A) as proposed. This amendment accommodates data center arrangements with multiple production sites, rather than reflecting only the traditional arrangement where one site is considered "primary" and another site is treated distinctly as a backup site. A designated FMU will still be required, however, to maintain a minimum of two locations that are sufficiently geographically distant from each other to have distinct risk profiles. Consistent with the Board's explanation when it adopted the current text of Regulation HH in 2014, the Board noted in the NPRM that it would consider sites to have "distinct risk profiles" if, for example, they are not located in areas that would be susceptible to

the same severe weather event (*e.g.*, the same hurricane zone) or on the same earthquake fault line. These sites would likely also have distinct power and telecommunications providers and be operated by geographically dispersed staff.

2. Recovery and resumption—Section 234.3(a)(17)(viii)(B)-(C)

a) Summary of Comments

Two commenters suggested that the Board incorporate into the text of Regulation HH the Board's statement in the NPRM that the recovery time objectives set forth in § 234.3(a)(17)(vii)(B)-(C) (renumbered as § 234.3(a)(17)(viii)(B)-(C)) should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.[45] One of these commenters expressed the concern that, absent clarification of the text of Regulation HH, a designated FMU could be required under Regulation HH to resume critical operations in an untrusted state in order to comply with the recovery time objectives.

b) Final Rule

The Board is adopting this section as proposed, without substantive change from the previous version of the rule. Regulation HH requires a designated FMU to have a business continuity *plan* that is *designed to enable* the designated FMU to meet these objectives. The Board reiterates that the recovery time objectives should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.

Since the Board established these requirements in Regulation HH, the two-hour recovery time objective has been a particular area of focus during bilateral discussions with Board-supervised designated FMUs, as well as in broader domestic and international fora, specifically in the context of extreme cyber events. At the center of those discussions is the balance between

[45] *See* 87 FR 60314, 60320 (Oct. 5, 2022).

(i) timely recovery and resumption of critical operations and (ii) appropriate assurance that critical operations are restored to a trusted state. The Board continues to believe it is imperative to financial stability that a designated FMU be able to recover and resume its critical operations and services quickly after disruptive events, both physical and cyber, and to complete settlement by the end of the day of the disruption. In related discussions with Board-supervised designated FMUs, and supported by provisions in the CPMI-IOSCO Cyber Guidance, Board staff has emphasized that recovery time objectives are necessary and critical targets around which plans, systems, and processes should be designed.[46] However, these recovery time objectives should not be interpreted as a requirement for a designated FMU to resume operations in a compromised or otherwise untrusted state.

Threats to designated FMUs' operations continue to evolve, and the Board expects that a designated FMU will update on an ongoing basis the scenarios in its plan to reflect evolving threats. The Board also expects that a designated FMU will seek and implement solutions that are designed to enable it to meet its recovery and resumptions objectives. For many types of disruptive scenarios, technologies and methods already exist to enable a designated FMU to recover and resume operations within two hours of the disruption. For example, if an earthquake damages a designated FMU's infrastructure and disrupts operations at one data center, the

[46] For example, paragraph 6.2.2 of the Cyber Guidance notes that the objectives for resuming operations set goals for, ultimately, the sound functioning of the financial system, which should be planned for and tested against. It further notes the criticality of the recovery and resumption objectives under Principle 17, Key Consideration 6 of the PFMI, while also acknowledging that financial market infrastructures should exercise judgment in effecting resumption so that risks to itself or its ecosystem do not thereby escalate. For additional details, see CPMI-IOSCO, *Guidance on Cyber Resilience for Financial Market Infrastructures* (June 2016) at section 6, https://www.bis.org/cpmi/publ/d146.htm ("Response and Recovery").

designated FMU may continue to operate from or fail over to another location that is outside the earthquake radius.

The Board recognizes, however, that certain threats to designated FMUs' operations, as well as the technology to mitigate those threats, are continually evolving. In areas where threats and technology are still evolving, such as is the case for extreme cyberattacks (*e.g.*, where significant data loss or corruption occurs across its data centers), the Board recognizes that a designated FMU will need to take a holistic approach that integrates protective, detective, and containment measures with response, recovery, and resumption solutions. The Board continues to expect that a designated FMU's business continuity planning will be a dynamic process in which the designated FMU works on an ongoing basis to update its plan to recover and resume operations in light of these evolving threats. Federal Reserve supervisors will also continue to work with designated FMUs through the supervisory process as designated FMUs identify reasonable approaches to prepare for and recover from such attacks. As development of adequate solutions for extreme cyberattacks continues, designated FMUs should also plan for contingency scenarios in which planned recovery and resumption objectives cannot be achieved. Planning for such scenarios would be in accordance with national policies aimed at improving the cybersecurity posture of U.S. critical infrastructures.[47]

[47] *See, e.g.*, Presidential Policy Directive/PPD-21, *Critical Infrastructure Security and Resilience* (Feb. 12, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

3. Reestablishment of availability after a disruption to the designated FMU's critical operations or services—Section 234.3(a)(17)(viii)(D)

a) Summary of Comments

One commenter expressed support for the proposal's requirement that a designated FMU have plans in place regarding reconnection to its participants following a cybersecurity disruption. Another commenter indicated that the criteria and processes for reconnection should be risk-based to account for the fact that a reconnection process may not be necessary for all disruptions or that aspects of such a process may not be needed in all cases. Another commenter suggested removing the term "reconnection" because not all disruptions result in a disconnection, thus a reconnection may not be required. This commenter suggested revising proposed § 234.3(a)(17)(viii)(D) to use the phrase "resumption of access" rather than "reconnection," and to specify that resumption of access to the designated FMU includes resumption of access to relevant functionalities. The commenter noted that, in a cyberattack scenario, in addition to disconnection, risk mitigants might include limiting or restricting a participant's access to the designated FMU or a particular functionality.

b) Final Rule

The Board has amended the text of proposed § 234.3(a)(17)(viii)(D) to require a designated FMU's business continuity plan to set out criteria and processes by which the designated financial market utility will "reestablish availability" for "affected" participants and other entities following a disruption to the designated FMU's critical operations or services.[48] In

[48] The NIST definitions of "availability" and "disruption" are consistent with the final rule. The NIST glossary, which can be found at https://csrc.nist.gov/glossary, defines "availability" as "timely, reliable access to data and information services for authorized users" and "disruption" as "an unplanned event that causes an information system to be inoperable for a length of time (*e.g.*,

the NPRM, the Board noted that it would consider a disruption to a designated FMU's critical operations or services broadly as a form of "disconnection" to external parties. However, some disruptions may not, as a technical matter, result in a designated FMU severing a participant's or other entity's connection to the designated FMU.

The Board believes that the term "reestablish availability" better captures the Board's expectations for designated FMUs. Proposed § 234.3(a)(17)(viii)(D) was intended to emphasize the importance of *ex ante* criteria and processes addressing when and how a designated FMU will make itself available to participants and other entities after a disruption causes the designated FMU's critical operations or services to become unavailable—regardless of whether there is a technical disconnection. This would include situations, as noted in the NPRM, in which a designated FMU deliberately takes itself offline such that participants cannot access its services (*e.g.*, if it experiences a major cyberattack that it needs to contain); it would also include situations where a designated FMU becomes unavailable due to another type of external event (*e.g.*, if its production site loses power due to a severe weather event in its region). In such situations, there may be a gap in availability, but not a disconnection by the designated FMU of participants or other entities from its services. The Board has also clarified that a designated FMU's criteria and processes should address resumption of availability to "affected" participants and other entities.

For the reasons discussed in section III.A, *supra*, the Board has not referred to a risk-based and proportionate approach in the final rule. Nevertheless, the Board recognizes that the

---

minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction)." https://csrc.nist.gov/glossary, defines "availability" as "timely, reliable access to data and information services for authorized users" and "disruption" as "an unplanned event that causes an information system to be inoperable for a length of time (*e.g.*, minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction)."

way in which a designated FMU applies its criteria and processes for reestablishing access may differ from one type of disruption to another. Some disruptions may be more straightforward and pose little risk to participants or other entities, while others may present greater risk of contagion. Given the current threat landscape and the ability for malware to spread, the Board believes it is crucial for a designated FMU to balance the need to quickly recover and resume its critical operations against the risk of contagion to its ecosystem should it resume operations in a compromised or otherwise untrusted state. For cyber incidents, it is particularly important for a designated FMU to be prepared to assure its participants, other connected entities, and regulator(s) that it has achieved an uncompromised and trusted state.[49] A designated FMU should consider establishing a phased approach to reestablishing access, transaction testing with selected participants, and heightened monitoring for an appropriate period of time after reestablishing access.

4. Business continuity testing and review—Section 234.3(a)(17)(viii)(E)-(F)

a) Summary of Comments

Two commenters noted that there may be circumstances in which recovery within two hours following disruptive events is not currently possible. One commenter expressed concern specifically with respect to § 234.3(a)(17)(viii)(E)(2), which proposed to require a designated FMU to demonstrate that its solutions for data recovery and reconciliation would enable it to meet its recovery and resumption objectives, even in case of extreme circumstances, including in the event of data loss or data corruption. That commenter encouraged the Board to amend proposed § 234.3(a)(17)(viii)(E)(2) to recognize the ever-evolving nature of cyber-threats and solutions to address them. Specifically, the commenter recommended that

[49] A designated FMU might consider leveraging third-party experts to verify its remediation efforts.

§ 234.3(a)(17)(viii)(E)(2) be amended to require a designated FMU, in consultation with its supervisors, to identify reasonable approaches to prepare for and recover from extreme cyber-attacks.

The Board did not receive comments on the proposed requirements for business continuity testing and review in § 234.3(a)(17)(viii)(E)(1), (E)(3), or (F).

b) Final Rule

The Board recognizes the ever-evolving nature of cyber threats and acknowledges that there are certain cyber scenarios which may result in extreme data loss or data corruption for which the designated FMU may not be able to demonstrate that its solutions for data recovery and data reconciliation enable it to meet the recovery and resumption objectives under § 234.3(a)(17)(viii)(B)-(C). The Board has therefore amended the final rule text in § 234.3(a)(17)(viii)(E)(2), and made conforming edits in § 234.3(a)(17)(viii)(E)(1) and (3), to clarify that a designated FMU's testing should assess the capability of its systems and the effectiveness of its procedures for data recovery and data reconciliation to meet the recovery and resumption objectives under § 234.3(a)(17)(viii)(B) and (C), even in case of extreme circumstances, including in the event of data loss or data corruption.

Designated FMUs should continue to plan for and test extreme scenarios from which they may need to recover, including wide-scale and major disruptions. Scenario testing should include functional testing of the designated FMU's ability to recover and resume settlement in the case of extreme cyber-based scenarios that cause data loss or data corruption. In some circumstances, a designated FMU may not be able to demonstrate that it can recover and resume operations within two hours, or complete settlement by end of day. The designated FMU should be able to demonstrate to supervisors, however, that (1) it is assessing the capability of its systems and effectiveness of its procedures against its recovery, resumption, and settlement

objectives; and (2) it has an understanding of the circumstances in which it may not be able to recover and resume critical operations and services within two hours following disruptive events or complete settlement by the end of the day. The designated FMU should also be able to demonstrate that it is working to increase the capability of its systems and effectiveness of its procedures to be able to meet those objectives in the future. The Board reiterates that Federal Reserve supervisors will continue to work with designated FMUs through the supervisory process as designated FMUs identify reasonable approaches to prepare for and recover from extreme cyber-attacks.

F. Third-party risk management

The Board expects a designated FMU to conduct its activities—whether conducted directly by the designated FMU or through a service provider—in a safe and sound manner.[50] Accordingly, the Board proposed to establish third-party risk management requirements in § 234.3(a)(17)(ix). The Board proposed these requirements because of the importance of ensuring that a designated FMU's activities do not become less safe when they are outsourced to third parties and because of the importance of managing operational risk associated with third-party relationships, including "supply chain risk."[51]

---

[50] The Board believes that this expectation is consistent with section 807(b) of the Dodd-Frank Act, which provides each Supervisory Agency of a designated FMU with authority to examine the provision of any service integral to the operation of the designated FMU for compliance with applicable law, rules, orders, and standards to the same extent as if the designated FMU were performing the service on its own premises. 12 U.S.C. 5466(b).

[51] Supply chain risk encompasses the potential for harm or compromise to a designated FMU that arises as a result of security risks from its third parties' subcontractors or suppliers, as well as the subcontractors' or suppliers' supply chains, and their products or services (including software that may be used by the third party or the designated FMU). This definition is consistent with NIST's definition of "supply chain risk" in the NIST computer-security incident handling guide. *See* NIST, *Computer Security Incident Handling Guide* (Special Publication

Specifically, the Board proposed to add a definition of "third party" in § 234.2(n), and to add § 234.3(a)(17)(ix) regarding the management of risks associated with third-party relationships. In § 234.2(n), the Board proposed to define "third party" as "any entity with which a designated FMU maintains a business arrangement, by contract or otherwise."[52] For purposes of proposed § 234.3(a)(17)(ix), the Board noted that it would consider third-party relationships to include vendor relationships for products such as software and arrangements for any services that third parties perform for a designated FMU.

In § 234.3(a)(17)(ix), the Board proposed to require a designated FMU to have systems, policies, procedures, and controls that effectively identify, monitor, and manage risks associated with third-party relationships. Additionally, for any service that is performed for the designated FMU by a third party, a designated FMU's systems, policies, procedures, and controls would need to ensure that risks are identified, monitored, and managed to the same extent as if the designated FMU were performing the service itself.[53]

800-61, rev. 2), https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf. The Board identified supply chain risk as a threat on which the Board is focused in its report on cybersecurity and financial system resilience. *See* Board of Governors of the Federal Reserve System, *Report to Congress: Cybersecurity and Financial System Resilience Report* (September 2021), https://www.federalreserve.gov/publications/files/cybersecurity-report-202109.pdf.

[52] This definition was consistent with the definition of "third-party relationship" in then-proposed interagency guidance for banking organizations on third-party relationships. *See* 86 FR 38182, 38186–87 (July 19, 2021). The Board explained in the NPRM that the Board viewed the requirements of proposed § 234.3(a)(17)(ix) as broadly consistent with the proposed interagency guidance. The Board, OCC, and FDIC have since adopted final *Interagency Guidance on Third-Party Relationships: Risk Management*. 88 FR 37920 (June 9, 2023). The Board continues to believe that the final amendments to Regulation HH remain broadly consistent with the final interagency guidance. In examining designated FMUs under Regulation HH, Board examiners will continue to reference guidance on third-party risk management.

[53] As noted in the NPRM, the Board believes that where a designated FMU outsources the provision of services to a third party, the designated FMU retains the responsibility for meeting the risk-management standards in Regulation HH.

In § 234.3(a)(17)(ix)(A)-(B), the Board proposed specific requirements for three components of third-party risk management: risk assessments, information-sharing arrangements, and business continuity management and testing. In § 234.3(a)(17)(ix)(A), the Board proposed to require a designated FMU to regularly conduct risk assessments of its third-party relationships and establish, as appropriate, information-sharing arrangements with third parties. In § 234.3(a)(17)(ix)(B), the Board proposed to require a designated FMU to include third parties in its business continuity management and testing, as appropriate.[54]

1. Definition of third-party risk; identification, monitoring, and management of risks associated with third-party relationships—Section 234.2(n); Section 234.3(a)(17)(ix)

a) Summary of Comments

Two commenters supported the addition of the third-party risk management rule to Regulation HH, but one of these commenters suggested the rule incorporate concepts of proportionality and criticality. Two commenters expressed concern with the scope of the definition of "third party." These commenters suggested narrowing the definition in a number of ways. One commenter suggested distinguishing between services the commenter considered "outsourced" and other third-party services. One commenter noted that the proposed definition may unintentionally capture entities with which a designated FMU has a business relationship, such as participants in a designated FMU and employees, but which it does not treat as traditional service-providing vendors. One commenter suggested that the "third party" definition

[54] In the final rule, the Board has reorganized risk assessment, information sharing, and business continuity management and testing into separate subsections (A), (B), and (C) of § 234.3(a)(17)(ix), respectively. The headings used in this **Supplementary Information** refer to these reorganized subsections.

should include only entities that could have a material impact on the designated FMU's designated activities.

One commenter suggested § 234.3(a)(17)(ix) be amended to permit the designated FMU to have risk-based systems, policies, procedures, and controls and to be flexible in managing third party risk. Another commenter explained that a designated FMU should be able to apply its most stringent risk management controls to third parties that provide services essential to performing the services for which the FMU was designated as systemically important. Both of these commenters also provided comments to the more specific requirements set forth in proposed § 234.3(a)(17)(ix)(A)-(B), which are addressed in sections III.F.2 and III.F.3, *infra*.

Finally, these commenters noted that the definition of third party would include central banks and other entities that may be unable or unwilling to establish formal information-sharing relationships or participate in a designated FMU's business continuity management and testing. Both commenters suggested excluding central banks from the definition, and one commenter recommended narrowing the definition by expressly excluding real-time gross settlement systems and their operators from the definition of "third party."

b) Final Rule

After considering the comments received, the Board has made one modification to the definition of "third party." Additionally, the Board is adopting as proposed the risk-management standards requirement set forth in the introductory portion of § 234.3(a)(17)(ix), but the Board has amended the specific requirements set forth in proposed § 234.3(a)(17)(ix)(A)-(B) to more expressly recognize that not all third parties present the same risk to a designated FMU.

As discussed in the NPRM, products and services provided by third parties can include a wide variety of arrangements, from heating, ventilation, and air conditioning (often referred to as HVAC) services that support the physical infrastructure of a designated FMU to technology

platforms or financial risk management modeling that are essential to executing a designated FMU's payment, clearing, or settlement activities. The Board does not believe it is appropriate to narrow the definition of third party to vendor, outsourcing, or other types of arrangements for purposes of the Board's third-party risk-management standards. Doing so could result in third-party risks being overlooked. The Board is concerned that limitations to "outsourced" or "traditional vendor" activities could result in inconsistent treatment of third parties, depending on how a particular designated FMU decides to categorize various third-party relationships. Moreover, the Board has observed that operational risk, and in particular cyber risk, has the potential to arise from unexpected sources, which may not be considered outsourced or even directly related to a designated FMU's critical operations or services. Thus, the Board believes that a designated FMU's systems, policies, procedures, and controls should address third parties more broadly.

A broad definition of third party does not mean, however, that the Board expects a designated FMU to address all third parties in the same manner. Although the Board, for the reasons described in section III.A, *supra*, has not expressly referred to a risk-based and proportionate approach in the final rule, the Board believes that § 234.3(a)(17)(ix) is consistent with such an approach. As the Board stated in the NPRM, a designated FMU should adopt risk management practices that are commensurate with the level of risk posed by its third-party relationships, as identified through the risk assessments it conducts.

While the Board generally believes a broad definition of third party is appropriate, the Board has, in response to comments, clarified in the final rule that relationships between a designated FMU and its participants are not "third-party" relationships when the participant is

acting in that capacity only.[55] If a participant maintains other relationships with a designated FMU – such as acting as a provider of pricing data, financial risk modeling services, liquidity, or asset custody services – the participant would be within the scope of the definition of "third party" as it relates to its other business arrangements with the designated FMU.[56]

2. Assessment of third party risk – Section 234.3(a)(17)(ix)(A)

a) Summary of Comments

As discussed in section III.F.1, commenters raised concerns about the scope of the definition of third party. As an alternative to definitional changes, one commenter suggested that the requirement to conduct risk assessments could apply broadly, but that specific information-sharing and business continuity testing requirements should apply only to third parties that provide critical services. Comments on the information-sharing and business continuity management and testing requirements are discussed in section III.F.3, *infra*.

b) Final Rule

The Board is adopting the risk assessment requirement in § 234.3(a)(17)(ix)(A) substantially as proposed but has moved the information sharing requirement to

[55] The Board also does not consider the relationship between a designated FMU and an employee to be a third-party relationship.

[56] The Board acknowledges that recent interagency guidance for banking organizations does not categorically exclude customer relationships from the scope of "business arrangements" within the scope of that guidance. 88 FR at 37922. In adopting the final interagency guidance, the agencies explained that some business relationships may incorporate elements or features of a customer relationship. Whereas banking organizations may enter into different types of arrangements, designated FMUs' arrangements with their participants are standardized and governed by a uniform set of terms applicable to each participant or class of participants, and risk management of participants is addressed in another section of Regulation HH. Specifically, § 234.3(a)(18) of Regulation HH requires a designated FMU to have objective, risk-based, and publicly disclosed criteria for participation; monitor compliance with its participation requirements on an ongoing basis; and have the authority to impose risk controls on a participant in situations where the designated FMU determines the participant poses heightened risk to the designated FMU. 12 CFR 234.3(a)(18).

§ 234.3(a)(17)(ix)(B) (and, consequently, the business continuity management and testing requirement to § 234.3(a)(17)(ix)(C)). To assess risk levels of third parties and monitor any changes in these risk levels that may affect a designated FMU and its ecosystem, the Board expects the designated FMU to regularly conduct risk assessments for each third party with which it maintains a business relationship. The Board expects that a designated FMU could incorporate a risk-based approach to prioritizing and determining the frequency and scope of risk assessments.

In general, and as discussed in the NPRM, the Board expects a designated FMU to take a rigorous and comprehensive approach to identifying, monitoring, and managing risks associated with third-party relationships. To do this effectively, it would be prudent for the designated FMU to understand *ex ante* any risks associated with the third party, including details on the services or products the third party will provide and the security controls and business continuity planning that the third party has in place. Before entering into a third-party relationship, the designated FMU should have a plan in place to address how it will effectively identify, monitor, and manage the relationship and its associated risks, in order to ensure that the designated FMU can continue to meet the risk-management requirements in Regulation HH.

3. Information sharing arrangements and business continuity and testing – Section 234.3(a)(17)(ix)(B)-(C)

a) Summary of Comments

Two commenters raised concerns about the requirement to enter into information-sharing arrangements with third parties and include third parties in business continuity and testing, as appropriate. One of the commenters suggested that, in lieu of narrowing the proposed definition of "third party," the Board could apply information-sharing and business continuity management and testing requirements only to third parties that provide critical services. That commenter also

requested further clarification with respect to any specific expectations or relevant objectives in connection with information-sharing arrangements and business continuity management and testing.

The same commenters noted that a designated FMU may not have the negotiating power to require certain third parties to enter into information-sharing arrangements or participate in the designated FMU's business continuity management and testing.[57] One of the commenters also raised concerns that third parties outside the United States could have limitations on their ability to share information with a designated FMU. To address these types of concerns, one commenter suggested that a designated FMU could implement alternative risk mitigants. For example, if a telecommunication provider would not enter into an information-sharing arrangement, the commenter suggested that a designated FMU could have redundant or diverse telecommunication channels.

The Board received a comment outside the scope of the proposal. The commenter noted that several third parties provide services to multiple designated FMUs and foreign systemically important FMIs. The commenter suggested that the Board and its foreign counterparts arrange scenario exercises involving designated FMUs and foreign FMIs. The commenter also recommended that the Board evaluate whether to have direct or collective oversight over certain third parties.

b) Final Rule

The Board is adopting § 234.3(a)(17)(ix)(B) and (C) with two substantive revisions in response to comments received. In addition, the Board has made structural changes to the rule

[57] One commenter proposed that the Board require the Federal Reserve Banks to provide designated FMUs with necessary information for the designated FMU to perform its third-party risk management.

text: the information-sharing requirement has been moved from proposed § 234.3(a)(17)(ix)(A) to § 234.3(a)(17)(ix)(B) and the business continuity management and testing requirement in proposed § 234.3(a)(17)(ix)(B) has been moved to new § 234.3(a)(17)(ix)(C).

First, the Board has amended the information-sharing and business continuity management and testing requirements to apply only with respect to third parties that provide services material to any of the designated FMU's critical operations or services. The Board believes that this limitation strikes an appropriate balance between effective risk management and the efficient use of resources by designated FMUs. A designated FMU should use the risk assessments conducted pursuant to final rule § 234.3(a)(17)(ix)(A) to inform its determinations of which third parties are in scope for purposes of § 234.3(a)(17)(ix)(B)-(C).

Second, the Board has amended the business continuity management and testing requirement to accommodate more clearly approaches to business continuity management and testing that do not include the participation of each third party in a designated FMU's testing. Specifically, the final rule provides that a designated FMU must "address" (rather than "include") in its business continuity management and testing, as appropriate, third parties that provide services material to any of the designated FMU's critical operations or services. The Board recognizes that there are effective approaches to testing that do not involve participation of a third party, such as planning for alternatives to be used in the event of a third party's unavailability. A designated FMU is expected to determine, through internal risk analysis, an appropriate way to address each covered third party, in business continuity management and testing, keeping in mind the overall requirement in § 234.3(a)(17)(ix) that the designated FMU effectively identify, monitor, and manage risks associated with third-party relationships.

The final rule, like the proposed rule, continues to apply an "as appropriate" qualification to the provisions related to information-sharing arrangements and business continuity management and testing. It does not set forth prescriptive requirements that a designated FMU must follow in all circumstances. The Board does not believe that prescriptive requirements would be appropriate, in light of different facts and circumstances a designated FMU may face with respect to each of its covered third parties. A designated FMU should consider what is appropriate in accordance with the risk-management standards articulated in the introductory portion of § 234.3(a)(17)(ix) and the risk assessments it conducts pursuant to § 234.3(a)(17)(ix)(A).

With respect to information-sharing arrangements, a designated FMU should conduct appropriate due diligence on third parties and ensure it obtains the information necessary to appropriately identify, monitor, and manage third-party risk. Information-sharing arrangements should include, where necessary, expectations related to when the designated FMU will be notified of material operational incidents or outages. They should also include, where appropriate, expectations with respect to information regarding the third party's information security controls, operational resilience objectives and capabilities, the third-party's arrangements with its own vendors, and changes in security controls at the third party. Consistent with a risk-based approach, a designated FMU should consider heightened requirements where there is higher risk. For example, with certain third parties that are essential to its critical operations and services, a designated FMU might require mandatory approval from the designated FMU before the service provider may outsource any material elements of its service to another party, in order to manage supply chain risks.

A designated FMU would generally be expected to make reasonable efforts to enter into contractual information-sharing arrangements, given the application of § 234.3(a)(17)(ix)(B) to third parties that provide services material to the designated FMU's critical operations or services. The Board, however, understands that there may be circumstances in which a designated FMU may not be able to negotiate a contractual information sharing arrangement with certain third parties or all of the designated FMU's desired terms. For example, utility operators such as electricity providers, as well as central banks or other operators of FMIs, may have particular needs for uniformity in how they interact with participants and customers.

In such situations, a designated FMU should consider whether it is appropriate to rely on non-contractual arrangements or other risk mitigants. In some cases, such as with central banks, the designated FMU may appropriately rely on informal information-sharing arrangements or, where available, other factors that may mitigate the risk associated with the lack of a contractual arrangement. For example, a designated FMU could consider the availability of public information about a third party or consider whether the designated FMU has sufficient contingency arrangements that would allow the designated FMU to continue to carry out its critical operations and services in a safe and sound manner in the absence of contractual information-sharing arrangements. A designated FMU might also consider the existence of backups, redundant services, or other means of managing third-party risk. If a designated FMU cannot with confidence ascertain and demonstrate that informal arrangements or other mitigants are sufficient, the designated FMU should consider whether it is appropriate to transition to an alternative third party, if available, or choose to keep a service in-house.

The Board expects that a designated FMU would evaluate the sufficiency of its business continuity arrangements with a third party in light of how the designated FMU addresses the

third party in its business continuity management and testing. In some circumstances, a designated FMU may determine that it is appropriate for a third party to participate directly in the designated FMU's scenario exercises to ensure that the designated FMU can effectively manage any instances in which the third party experiences an incident causing disruption or material degradation to the designated FMU's critical operations or services. For example, where a cyberattack on a third party could impair the third party's ability to enable a designated FMU to fulfill its obligations on time, it may be necessary for the designated FMU to include the third party in scenario exercises to enable the designated FMU to be prepared to react, such as by switching to a contingency plan. If a designated FMU determines that it is essential for a third party to participate in business continuity testing, the Board would, in line with the discussion above regarding information-sharing arrangements, generally expect the designated FMU to make reasonable efforts to require that participation by contract. It may be reasonable in some circumstances for a designated FMU to rely on non-contractual arrangements with third parties, such as central banks, to participate in the designated FMU's business continuity planning.

In other circumstances, a designated FMU may have contingencies in place such that participation by a particular third party in business continuity testing is not essential. If participation is not essential, a designated FMU should consider whether its information-sharing arrangements or other available sources of information afford the designated FMU with access to sufficient information to effectively address the third party in business continuity testing. The sufficiency of information may depend on the services provided by the third party and a designated FMU's ability to conduct critical operations and services safely and soundly in contingency scenarios without the third party. A designated FMU should consider the third party's business continuity planning in any risk assessment of the third party that the designated

FMU completes, and, where appropriate, the designated FMU should include information about a third party's own business continuity planning in information-sharing arrangements it establishes with a third party.

G. Technical revisions

1. Definition of operational risk

a) Proposed Rule

In § 234.2(h), the Board proposed to add "operational risk" as a defined term in Regulation HH. The Board proposed to define this term as "the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the designated financial market utility."

b) Summary of Comments

The Board received one comment that supported the proposed definition of operational risk.

c) Final Rule

The Board is adopting the definition of "operational risk" as proposed. This definition is consistent with the definition of operational risk in the PFMI and the Board's definition in part I of the *Federal Reserve Policy on Payment System Risk* (PSR policy).[58] In the supplementary information of its 2014 notice of proposed rulemaking, the Board had provided this definition of operational risk when it proposed amendments to Regulation HH based on the PFMI.[59]

---

[58] Part I of the PSR policy sets out the Board's views, and related standards, regarding the management of risks in financial market infrastructures, including those operated by the Reserve Banks. The Board concurrently amended the risk-management standards in Regulation HH and revised part I of the PSR policy based on the PFMI in 2014. The PSR policy is available at https://www.federalreserve.gov/paymentsystems/files/psr_policy.pdf.

[59] 79 FR 3666, 3683 (Jan. 22, 2014).

2. Definition of critical operations and critical services

a) Proposed Rule

In § 234.2(d), the Board proposed to add "critical operations" and "critical services" as defined terms in Regulation HH, in order to streamline references to these terms. Under the proposal, these terms were defined as "any operations or services that the designated financial market utility identifies under 12 CFR 234.3(a)(3)(iii)(A)."

b) Summary of Comments

The Board received one comment on the definition of critical operations and critical services, which was supportive of the revision.

c) Final Rule

The Board is adopting the definition of critical operations and critical services as proposed. Under § 234.3(a)(3)(iii)(A), a designated FMU must identify its critical operations and services related to payment, clearing, and settlement for purposes of developing its integrated plans for recovery and orderly wind-down. The Board's amendments to § 234.3(a)(17), related to review and testing, incident management and planning, and business continuity management planning, refer to a designated FMU's critical operations and/or services in multiple places. Amending Regulation HH to include definitions of "critical operations" and "critical services" clarifies that the critical operations or services that the designated FMU should consider under paragraph (a)(17) are the same set of critical operations and services that the designated FMU has identified under paragraph (a)(3).

3. Cross-reference to "other entities" identified in § 234.3(a)(3) on comprehensive management of risk

a) Proposed Rule

The Board proposed to streamline and replace the reference to "financial market utilities and trade repositories, if any" in § 234.3(a)(17)(ii) with the phrase "relevant entities such as those referenced in paragraph (a)(3)(ii)." In connection with this, the Board proposed to include "trade repositories" in the list of entities listed under § 234.3(a)(3)(ii).[60]

b) Summary of Comments

One commenter had no objection to the addition of the term "trade repositories" to § 234.3(a)(3)(ii), but suggested changing the term "relevant entities" as used in § 234.3(a)(17)(ii) to "identified entities." The commenter noted that change would allow the word "relevant" to be used elsewhere in the rule when discussing the entities referenced in § 234.3(a)(17)(ii)

c) Final Rule

The Board has adopted the proposed revisions to § 234.3(a)(3)(ii) and § 234.3(a)(17)(ii) but has removed the word "relevant" from the latter revision. Upon review, the Board believes that the reference to entities listed in § 234.3(a)(3)(ii) is sufficiently clear without including a modifier like "relevant" or "identified." The Board believes that, as adopted, § 234.3(a)(17)(ii) is consistent with the requirement under subparagraph (a)(3)(ii) for the designated FMU to identify, measure, monitor, and manage the material risks that it poses due to interdependencies with other entities, such as other FMUs, settlement banks, liquidity providers, and service providers.

[60] Because of the differences in the definition for financial market infrastructure in the PFMI, which includes trade repositories, and the definition of FMU in the Dodd-Frank Act, which does not, the Board had previously inadvertently excluded the reference to "trade repositories" in § 234.3(a)(3)(ii).

4. Operational capabilities to ensure high degree of security and operational reliability

a) Proposed Rule

Section 234.3(a)(17)(iii) requires a designated FMU to have "policies and systems" that are designed to achieve clearly defined objectives to ensure a high degree of security and operational reliability.

A designated FMU is implicitly required to have the operational capability to achieve these objectives. In § 234.3(a)(17)(iii), the Board proposed to make this requirement explicit by clarifying that a designated FMU must have "operational capabilities"—in addition to the existing reference to "policies and systems"—that are designed to achieve clearly defined objectives to ensure a high degree of security and operational reliability.

b) Summary of Comments

One commenter suggested removing the reference to "operational capabilities" in proposed § 234.3(a)(17)(iii) and instead adding a reference to "processes and controls," in addition to "policies and systems." The commenter noted this drafting would better align with the terminology used throughout Regulation HH.

c) Final Rule

Upon consideration of the comment, the Board has removed the term "operational capabilities" in proposed § 234.3(a)(17)(iii) and replaced it with "procedures and controls." This change aligns the language in § 234.3(a)(17)(iii) with terminology used elsewhere in Regulation HH. Regulation HH frequently uses the term "procedures and controls," and the Board believes the phrase achieves the suggested drafting consistency and the intended meaning.

The Board expects a designated FMU to establish clearly defined objectives to ensure a high degree of security and operational reliability; to have systems, procedures, and controls

designed to achieve these objectives; and to have policies, such as benchmarks, in place for the designated FMU to evaluate its systems' performance against these objectives.

5. Identify, monitor, and manage potential and evolving vulnerabilities and threats

a) Proposed Rule

Section 234.3(a)(17)(v) requires a designated FMU to have comprehensive physical, information, and cyber security policies, procedures, and controls "that address" potential and evolving vulnerabilities and threats. The Board proposed a technical change to clarify what it means to "address" potential and evolving vulnerabilities and threats. Specifically, the Board proposed to replace the phrase "that address" with the phrase "that enable the designated financial market utility to identify, monitor, and manage" potential and evolving vulnerabilities and threats.

b) Summary of Comments

One commenter supported the proposed change. No other comments were received in response to this proposed revision of § 234.3(a)(17)(v).

c) Final Rule

The Board is adopting the technical revision as proposed.

IV. Administrative Law Matters

A. Regulatory Flexibility Act Analysis

The Regulatory Flexibility Act (RFA) generally requires that, in connection with a final rulemaking, an agency prepare and make available a final regulatory flexibility analysis describing the impact of the final rule on small entities.[61] However, a final regulatory flexibility

[61] 5 U.S.C. 601 *et seq*.

analysis is not required if the agency certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

The Small Business Administration (SBA) has adopted size standards for determining whether a particular entity is considered a "small entity" for purposes of the RFA. The Board believes that the most appropriate SBA size standard to apply in determining whether a designated FMU is a small entity is the SBA size standard for financial transactions processing, reserve, and clearinghouse activities. Under this standard, a designated FMU is considered a small entity if its annual receipts are less than $47 million.[62] The Board includes the assets of all domestic and foreign affiliates in determining whether to classify a designated FMU as a small entity.[63] For the reasons described below and under section 605(b) of the RFA, the Board certifies that the final rule will not have a significant economic impact on a substantial number of small entities.[64]

In connection with the proposed rule, the Board stated that it did not believe that the proposal would have a significant economic impact on a substantial number of small entities. Nevertheless, the Board published and invited comment on an initial regulatory flexibility analysis of the proposal. No comments were received on the initial regulatory flexibility analysis.

---

[62] 13 CFR 121.201 (subsector 522320). Alternatively, the SBA size standards for (1) securities and commodities exchanges; (2) trust, fiduciary, and custody activities; or (3) international, secondary market, and all other nondepository credit intermediation activities could also apply to certain designated FMUs; these size standards are currently the same as the size standard for financial transactions processing, reserve, and clearinghouse activities (*i.e.,* annual receipts of less than $47 million). *Id.* (subsectors 523210, 523991, and 522299).

[63] 13 CFR 121.103.

[64] 5 U.S.C. 605(b).

The Board is finalizing amendments to Regulation HH that would affect the regulatory requirements that apply to designated FMUs other than derivatives clearing organizations registered with the CFTC and clearing agencies registered with the SEC. At present, the FSOC has designated eight FMUs as systemically important; two of these designated FMUs are subject to the Board's Regulation HH. The reasons and justification for the final rule are described above in more detail in this **Supplementary Information**.

The Board has considered whether to conduct a final regulatory flexibility analysis in connection with the final rule. However, the annual receipts of designated FMUs subject to this final rule exceed the $47 million threshold under which a designated FMU is considered a "small entity" under SBA regulations. Because the final rule is not likely to apply to any company with annual receipts of $47 million or less, it is not expected to apply to any small entity for purposes of the RFA. In light of the foregoing, the Board certifies that the final rule will not have a significant economic impact on a substantial number of small entities.

B. Competitive Impact Analysis

As a matter of policy, the Board conducts a competitive impact analysis in connection with any operational or legal changes that could have a substantial effect on payment system participants, even if competitive effects are not apparent on the face of the proposal. Pursuant to this policy, the Board assesses whether proposed changes "would have a direct and material adverse effect on the ability of other service providers to compete effectively with the Federal Reserve in providing similar services" and whether any such adverse effect "was due to legal differences or due to a dominant market position deriving from such legal differences." If, as a result of this analysis, the Board identifies an adverse effect on competition, the Board then

assesses whether the associated benefits – such as improvements to payment system efficiency or integrity – can be achieved while minimizing the adverse effect on competition.[65]

Designated FMUs are subject to the supervisory framework established under Title VIII of the Dodd-Frank Act. The final rule amends current Regulation HH operational risk-management standards for certain designated FMUs. At least one designated FMU that is currently subject to Regulation HH competes with the Fedwire®[66] Funds Service provided by the Reserve Banks.

Under the Federal Reserve Act, the Board has general supervisory authority over the Reserve Banks, including the Reserve Banks' provision of payment and settlement services. This general supervisory authority is more extensive in scope than the Board's authority over certain designated FMUs under Title VIII. In practice, Board oversight of the Reserve Banks goes beyond the typical supervisory framework for private-sector entities, including the framework provided by Title VIII. The Fedwire Funds Service and Fedwire Securities Service (collectively, Fedwire Services) are subject to the risk-management standards in part I of the PSR policy, including applicable principles from the PFMI as set forth in an appendix to the PSR policy. The Board is guided by its interpretation of the corresponding provisions of Regulation HH in its application of the risk management expectations in the PSR policy.[67]

One commenter expressed its appreciation for the Board's commitment to apply risk-management standards to the Fedwire Funds Service that are at least as stringent as those in

---

[65] *See Policies: The Federal Reserve in the Payments System* (issued 1984; revised 1990 and January 2001), https://www.federalreserve.gov/paymentsystems/pfs_frpaysys.htm.

[66] Fedwire is a registered service mark of the Reserve Banks. A list of marks related to financial service products that are offered to financial institutions by the Reserve Banks is available at FRBservices.org.

[67] *See* section I.B.1 of the PSR policy.

Regulation HH, but asked the Board to amend the appendix to the PSR policy to more closely align with Regulation HH. The commenter also requested that the Board revise the PSR policy to include the Reserve Banks' National Settlement Service (NSS), along with the Fedwire Services, as a service subject to the appendix of the PSR policy.

The Board recognizes the critical role that the Fedwire Services play in the financial system and, as noted in the proposal, the Board remains committed to applying risk-management standards to the Fedwire Funds Service that are at least as stringent as the Regulation HH standards that are applied to designated FMUs that provide similar services. At the same time, however, the Board continues to believe that a different level of detail is required for Regulation HH than for part I of the PSR policy. Regulation HH is an enforceable rule applicable to designated FMUs other than those supervised by the CFTC or SEC, so additional detail provides greater clarity on the Board's expectations. The PSR policy, on the other hand, is a policy statement that provides guidance about (as relevant here) the Board's exercise of its other supervisory or regulatory authority over other financial market infrastructures (including those operated by the Reserve Banks) or their participants.

The Board continues to believe that the current approach to the appendix to the PSR policy is consistent with the purpose of the document and the Board's long-standing supervisory approach under the PSR policy. In light of the Federal Reserve's oversight framework for the Fedwire Services, the Board does not believe that the amendments to Regulation HH will have any direct and material adverse effect on the ability of other service providers to compete with the Reserve Banks.

Finally, the Board does not believe that the exclusion of NSS from the list of Federal Reserve services subject to the appendix of the PSR policy has a direct and material effect on the

ability of other service providers to compete with the Reserve Banks. NSS provides services to a number of financial market infrastructures, but is not itself a competitor with other service providers, and in particular with any service providers to which Regulation HH applies.

C. Paperwork Reduction Act Analysis

In accordance with the Paperwork Reduction Act of 1995 (44 U.S.C. 3506; 5 CFR part 1320, Appendix A.1), the Board reviewed the final rule under the authority delegated to the Board by the Office of Management and Budget. As noted in the NPRM, for purposes of the Paperwork Reduction Act, a "collection of information" involves 10 or more respondents. Any recordkeeping, disclosure, or reporting requirement that is contained in a rule of general applicability or that is addressed to all or a substantial majority of an industry is presumed to involve 10 or more respondents (5 CFR 1320.3(c), 1320.3(c)(4)). Regulation HH applies to fewer than 10 persons, and these persons do not represent all or a substantial majority of the participants in payment, clearing, and settlement systems. Additionally, Regulation HH is not a rule of general applicability. Therefore, no collections of information under the Paperwork Reduction Act are contained in the final rule. The Board did not receive any comments on this analysis.

List of Subjects in 12 CFR Part 234

Banks, banking, Credit, Electronic funds transfers, Financial market utilities, Securities

Authority and Issuance

For the reasons set forth in the preamble, the Board is amending part 234 of chapter II of title 12 of the Code of Federal Regulations, as follows:

PART 234 – DESIGNATED FINANCIAL MARKET UTILITIES (REGULATION HH)

1. The authority citation for part 234 continues to read as follows:

Authority: 12 U.S.C. 5461 *et seq.*

2. Revise § 234.2 as follows:

§ 234.2 Definitions.

(a) *Backtest* means the *ex post* comparison of realized outcomes with margin model forecasts to analyze and monitor model performance and overall margin coverage.

(b) *Central counterparty* means an entity that interposes itself between counterparties to contracts traded in one or more financial markets, becoming the buyer to every seller and the seller to every buyer.

(c) *Central securities depository* means an entity that provides securities accounts and central safekeeping services.

(d) *Critical operations* and *critical services* refer to any operations or services that the designated financial market utility identifies under 12 CFR 234.3(a)(3)(iii)(A).

(e) *Designated financial market utility* means a financial market utility that is currently designated by the Financial Stability Oversight Council under section 804 of the Dodd-Frank Act (12 U.S.C. 5463).

(f) *Financial market utility* has the same meaning as the term is defined in section 803(6) of the Dodd-Frank Act (12 U.S.C. 5462(6)).

(g) *Link* means, for purposes of § 234.3(a)(20), a set of contractual and operational arrangements between two or more central counterparties, central securities depositories, or securities settlement systems, or between one or more of these financial market utilities and one or more trade repositories, that connect them directly or indirectly, such as for the purposes of participating in settlement, cross margining, or expanding their services to additional instruments and participants.

(h) *Operational risk* means the risk that deficiencies in information systems or internal processes, human errors, management failures, or disruptions from external events will result in the reduction, deterioration, or breakdown of services provided by the designated financial market utility.

(i) *Orderly wind-down* means the actions of a designated financial market utility to effect the permanent cessation, sale, or transfer of one or more of its critical operations or services in a manner that would not increase the risk of significant liquidity or credit problems spreading among financial institutions or markets and thereby threaten the stability of the U.S. financial system.

(j) *Recovery* means, for purposes of § 234.3(a)(3) and (15), the actions of a designated financial market utility, consistent with its rules, procedures, and other *ex ante* contractual arrangements, to address any uncovered loss, liquidity shortfall, or capital inadequacy, whether arising from participant default or other causes (such as business, operational, or other structural weaknesses), including actions to replenish any depleted prefunded financial resources and liquidity arrangements, as necessary to maintain the designated financial market utility's viability as a going concern and to continue its provision of critical services.

(k) *Securities settlement system* means an entity that enables securities to be transferred and settled by book entry and allows transfers of securities free of or against payment.

(l) *Stress test* means the estimation of credit or liquidity exposures that would result from the realization of potential stress scenarios, such as extreme price changes, multiple defaults, and changes in other valuation inputs and assumptions.

(m) *Supervisory Agency* has the same meaning as the term is defined in section 803(8) of the Dodd-Frank Act (12 U.S.C. 5462(8)).

(n) *Third party* means any entity, other than a participant of a designated financial market utility acting in that capacity, with which a designated financial market utility maintains a business arrangement, by contract or otherwise.

(o) *Trade repository* means an entity that maintains a centralized electronic record of transaction data, such as a swap data repository or a security-based swap data repository.

3. In § 234.3:

(a) Revise the section heading;

(b) Add the words "trade repositories," after the words "such as other financial market utilities," in paragraph (a)(3)(ii);

(c) Remove the word "following" and add in its place "after", in paragraph (a)(3)(iii)(G);

(d) Revise paragraph (a)(17); and

(e) Remove the word "following" and replace with the words "to reflect", in paragraph (a)(23)(v).

The addition and revisions read as follows:

§ 234.3 Standards for designated financial market utilities.

(a) * * *

(17) Operational risk. The designated financial market utility manages its operational risks by establishing a robust operational risk-management framework that is approved by the board of directors. In this regard, the designated financial market utility –

(i) Identifies the plausible sources of operational risk, both internal and external, and mitigates their impact through the use of appropriate systems, policies, procedures, and controls – including those specific systems, policies, procedures, or controls required pursuant to this

paragraph (a)(17) – that are reviewed, audited, and tested periodically and after major changes such that –

(A) The designated financial market utility conducts tests –

(*1*) In accordance with a documented testing framework that addresses, at a minimum, scope, frequency, participation, interdependencies, and reporting; and

(*2*) That assess whether the designated financial market utility's systems, policies, procedures, or controls function as intended;

(B) The designated financial market utility reviews the design, implementation, and testing of affected and similar systems, policies, procedures, and controls, after material operational incidents, including the material operational incidents described in paragraph (a)(17)(vi)(A) of this section, or after changes to the environment in which the designated financial market utility operates that could significantly affect the plausible sources or mitigants of operational risk; and

(C) The designated financial market utility remediates as soon as possible, following established governance processes, deficiencies in systems, policies, procedures, or controls identified in the process of review or testing;

(ii) Identifies, monitors, and manages the risks its operations might pose to other entities such as those referenced in paragraph (a)(3)(ii) of this section;

(iii) Has systems, policies, procedures, and controls that are designed to achieve clearly defined objectives to ensure a high degree of security and operational reliability;

(iv) Has systems that have adequate, scalable capacity to handle increasing stress volumes and achieve the designated financial market utility's service-level objectives;

(v) Has comprehensive physical, information, and cyber security policies, procedures, and controls that enable the designated financial market utility to identify, monitor, and manage potential and evolving vulnerabilities and threats;

(vi) Has a documented framework for incident management that provides for the prompt detection, analysis, and escalation of an incident, appropriate procedures for addressing an incident, and incorporation of lessons learned following an incident. This framework includes a plan for notification and communication of material operational incidents to identified relevant entities that ensures the designated financial market utility –

(A) Immediately notifies the Board, in accordance with the process established by the Board, when the designated financial market utility activates its business continuity plan or has a reasonable basis to conclude that –

(*1*) There is an actual or likely disruption, or material degradation, to any critical operations or services, or to its ability to fulfill its obligations on time; or

(*2*) There is unauthorized entry or a vulnerability that could allow unauthorized entry into the designated financial market utility's computer, network, electronic, technical, automated, or similar systems that affects or has the potential to affect its critical operations or services;

(B) Establishes criteria and processes providing for timely communication and responsible disclosure of material operational incidents to the designated financial market utility's participants and other relevant entities, such that –

(*1*) Affected participants are notified immediately of actual disruptions or material degradations to any critical operations or services, or to the designated financial market utility's ability to fulfill its obligations on time; and

(*2*) Participants and other relevant entities, as identified in the designated financial market utility's plan for notification and communication, are notified in a timely manner of material operational incidents described in paragraph (a)(17)(vi)(A) of this section, as appropriate, taking into account the risks and benefits of the disclosure to the designated financial market utility and such participants and other relevant entities;

(vii) Has business continuity management that provides for rapid recovery and timely resumption of critical operations and services and fulfillment of its obligations, including in the event of a wide-scale disruption or a major disruption;

(viii) Has a business continuity plan that –

(A) Incorporates the use of two sites providing for sufficient redundancy supporting critical operations that are located at a sufficient geographical distance from each other to have a distinct risk profile;

(B) Is designed to enable critical systems, including information technology systems, to recover and resume critical operations and services no later than two hours following disruptive events;

(C) Is designed to enable it to complete settlement by the end of the day of the disruption, even in case of extreme circumstances;

(D) Sets out criteria and processes by which the designated financial market utility will reestablish availability for affected participants and other entities following a disruption to the designated financial market utility's critical operations or services;

(E) Provides for testing, pursuant to the requirements under paragraphs (a)(17)(i)(A) and (a)(17)(i)(C) of this section, at least annually, of the designated financial market utility's

business continuity arrangements, including the people, processes, and technologies of the sites required under paragraph (a)(17)(viii)(A), such that –

(*1*) The designated financial market utility can demonstrate that it can run live production at the sites required under paragraph (a)(17)(viii)(A);

(*2*) The designated financial market utility assesses the capability of its systems and effectiveness of its procedures for data recovery and data reconciliation to meet the recovery and resumption objectives under paragraphs (a)(17)(viii)(B) and (a)(17)(viii)(C) of this section, even in case of extreme circumstances, including in the event of data loss or data corruption; and

(*3*) The designated financial market utility can demonstrate that it has geographically dispersed staff who can effectively run the operations and manage the business of the designated financial market utility; and

(F) Is reviewed, pursuant to the requirements under paragraphs (a)(17)(i)(B) and (a)(17)(i)(C) of this section, at least annually, in order to –

(*1*) Incorporate lessons learned from actual and averted disruptions; and

(*2*) Update scenarios and assumptions in order to ensure responsiveness to the evolving risk environment and incorporate new and evolving sources of operational risk; and

(ix) Has systems, policies, procedures, and controls that effectively identify, monitor, and manage risks associated with third-party relationships, and that ensure that, for any service that is performed for the designated financial market utility by a third party, risks are identified, monitored, and managed to the same extent as if the designated financial market utility were performing the service itself. In this regard, the designated financial market utility –

(A) Regularly conducts risk assessments of third parties;

(B) Establishes information-sharing arrangements, as appropriate, with third parties that provide services material to any of the designated financial market utility's critical operations or services; and

(C) Addresses in its business continuity management and testing, as appropriate, third parties that provide services material to any of the designated financial market utility's critical operations or services.

* * * * *

By order of the Board of Governors of the Federal Reserve System.

Ann E. Misback,
Secretary of the Board.