Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2020-SR-B-019, September 30, 2020

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

Findings

The Board of Governors of the Federal Reserve System's approach to cybersecurity supervision of Large Institution Supervision Coordinating Committee (LISCC) firms continues to evolve and can be enhanced. We determined that the Board can strengthen its governance of LISCC firm cybersecurity supervision. Over the past several years, the Board's Division of Supervision and Regulation (S&R) has undergone several structural changes affecting its governance of the cybersecurity supervision for LISCC firms. These structural changes have created a need to define the roles and responsibilities of the groups that are currently involved in LISCC cybersecurity supervision and planning. Additionally, the Board can better define how cybersecurity supervisory activities inform the governance and controls ratings of LISCC firms. Clarifying how weaknesses or deficiencies identified during cybersecurity supervision activities factor into these ratings can help the LISCC program better communicate its assessment regarding firms' cybersecurity posture.

Further, the LISCC program can enhance its approach to cybersecurity training. In addition, some cybersecurity examiners have difficulty obtaining training. The inability of cybersecurity examiners to keep their skills updated could affect their readiness to examine emerging cybersecurity risk areas and can adversely affect retention and recruitment. Finally, examiners would benefit from additional guidance and training on reporting cybersecurity incidents in the Federal Reserve System's designated repository. Absent clear guidance and training, users may not be consistently entering cybersecurity events into the repository, increasing the likelihood that the System may not be effectively and timely synthesizing information on cybersecurity incidents.

Recommendations

Our report contains recommendations designed to enhance the effectiveness of the Board's cybersecurity supervision of LISCC firms. In its response to our draft report, the Board concurs with our recommendations and outlines actions that have been or will be taken to address our recommendations. We will follow up to ensure that the recommendations are fully addressed.

Purpose

We conducted this evaluation to assess the effectiveness of the Board's and the Federal Reserve Banks' cybersecurity supervision approach for LISCC firms. The scope of our evaluation included applicable laws, regulations, policies, procedures, and agency practices related to the cybersecurity supervision of LISCC firms.

Background

S&R is responsible for leading the System's supervisory activities. The LISCC is chaired by the director of S&R and is responsible for overseeing the supervision of the largest, most systemically important financial institutions under the Board's purview.

Cybersecurity risks present significant and dynamic challenges to LISCC firms. Board and Reserve Bank staff supervise LISCC firms through a combination of horizontal examinations, firm-specific idiosyncratic examinations, and monitoring activities. The governance and controls core assessment program, one of four LISCC core assessment programs, is responsible for overseeing the supervision of LISCC firm information technology and cybersecurity risks, among other areas. The LISCC program's supervisory work culminates in an annual integrated assessment letter for each firm, which highlights key themes and supervisory concerns. It also culminates in annual ratings for three core assessment areas, including a governance and controls rating, under the Board's large financial institution rating system.