

Open Recommendations Made to the Board of Governors of the Federal Reserve System



We oversee the Board of Governors of the Federal Reserve System by conducting audits, evaluations, and inspections of the Board’s programs and operations and by making recommendations to improve economy, efficiency, and effectiveness.

Audits assess aspects of the economy, efficiency, and effectiveness of Board programs and operations and are conducted in accordance with *Government Auditing Standards*, which is issued by the comptroller general of the United States. Evaluations and inspections include program evaluations and statutorily mandated reviews of failed financial institutions supervised by the Board. Evaluations are generally focused on the effectiveness of specific programs or functions, and inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Evaluations and inspections are performed according to *Quality Standards for Inspection and Evaluation*, which is issued by the Council of the Inspectors General on Integrity and Efficiency.

Our audit, evaluation, and inspection reports explain why we conducted the review and the issues we found that should be corrected or improved, and they contain specific recommendations for agency corrective action. Table 1 shows, as of September 30, 2021, the total number and status of recommendations we made to the Board by calendar year, beginning with the first year for which recommendations remain open.

Table 1. Status of Recommendations for 2016–2021, as of September 30, 2021

Status	2016	2017	2018	2019	2020	2021
Recommendations	40	41	57	22	43	11
Open	1	6	9	9	13	11
Closed	39	35	48	13	30	0
Public recommendations	30	41	37	22	43	11
Open	1	6	4	9	13 ^a	11 ^a
Closed	29	35	33	13	30	0
Nonpublic recommendations	10	0	20	0	0	0
Open	0	0	5	0	0	0
Closed	10	0	15	0	0	0

Note: Some reports are restricted because they contain sensitive information. The recommendations from these reports are identified as nonpublic.

^a Only the recommendations that have been open for more than 12 months are reflected in the accompanying list of open recommendations.

This document provides a list of publicly available report recommendations we made to the Board that have been open for more than 12 months as of September 30, 2021, and their status. The status designations and their definitions are as follows:

- **Agency concurrence**—The Board stated that it plans to implement the recommendation.
- **Agency nonconcurrence**—The Board stated that it does not concur with the recommendation. We continue to believe the recommendation should be implemented and are working with the Board to reach a resolution.
- **Agency partial concurrence**—The Board stated that it does not agree with part of the recommendation. We continue to believe the recommendation should be fully implemented and are working with the Board to reach a resolution.
- **Agency action**—The Board reported that it has begun taking steps to implement the recommendation.
- **Partial implementation**—The Board reported that it has completed actions to close part of the recommendation and is taking steps to close the remaining aspects.
- **Verification in progress**—The Board reported that it has completed actions to fully close the recommendation. We are verifying that the actions address the recommendation.

For inquiries about the list of open recommendations, please contact oig.media@frb.gov or 202-973-5043.

Publicly Available Board Recommendations Open for More Than 12 Months

Report title	Issuance date	Recommendation	Recommendation status
2016 Audit of the Board's Information Security Program 2016-IT-B-013	11/10/2016	1. Work with the chief operating officer to perform a risk assessment to determine which aspects of an insider threat program are applicable to other types of sensitive Board information and develop and implement an agencywide insider threat strategy for sensitive but unclassified Board information, as appropriate.	Verification in progress
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing 2017-IT-B-009	04/17/2017	1. Reiterate to financial institutions the requirement to notify their primary regulator of the existence of new service relationships, and develop a process to periodically reconcile and refresh the listing of multiregional data processing servicer firms and technology service providers.	Agency action
2017 Audit of the Board's Information Security Program 2017-IT-B-018	10/31/2017	1. Ensure that <ol style="list-style-type: none"> a. an optimal governance structure for enterprise risk management is implemented that includes considerations for a chief risk officer or equivalent function. b. an enterprise risk management strategy is used to maintain a risk profile for the Board. 	Verification in progress
		4. Ensure that the Board's enterprise architecture includes technologies managed by all divisions, and work with the chief operating officer to enforce associated review processes agencywide.	Verification in progress
		5. Develop and implement an agencywide identity, credential, and access management strategy that assesses current processes, provides a vision for the desired future state, and identifies plans to achieve that future state.	Verification in progress
		8. Develop, implement, and regularly update an information security continuous monitoring strategy that includes performance measures to gauge the effectiveness of related processes and provides agencywide security status.	Agency action
The Board's Organizational Governance System Can Be Strengthened 2017-FMIC-B-020	12/11/2017	10. Communicate and reinforce the Board of Governors' expectations of the chief operating officer and the heads of the enterprisewide administrative functions to all division directors and consider tools that will enable the Board of Governors to enhance the effectiveness of these functions, such as <ol style="list-style-type: none"> a. holding periodic meetings with the chief operating officer to discuss the administration of the agency and progress on administrative initiatives. b. identifying and implementing mechanisms to hold division directors accountable for their role in the administrative functions. 	Agency action

Report title	Issuance date	Recommendation	Recommendation status
2018 Audit of the Board's Information Security Program 2018-IT-B-017	10/31/2018	6. Develop and implement a process to assess the knowledge, skills, and abilities of Board staff with significant security responsibilities and establish plans to close identified gaps.	Agency action
The Board Can Strengthen Information Technology Governance 2018-IT-B-020	11/05/2018	2. Require divisions with embedded information technology units to inform the chief information officer of their information technology investment plans.	Agency action
		3. Require that all information technology investments align with the Board's enterprisewide architecture unless such information technology investments receive a waiver from the chief information officer.	Agency action
		4. Clarify and document the roles and responsibilities of the Board's information technology governance boards and committees and require division-level governance boards and committees to include the chief information officer, or their designee, as appropriate.	Agency action
The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency 2019-SR-B-013	09/25/2019	1. Issue internal guidance on the enforcement action issuance and termination processes that <ol style="list-style-type: none"> defines the general steps to take when issuing and terminating each type of enforcement action. clearly defines the roles and responsibilities of the parties involved in the processes. reflects any structural or process changes that result from recommendations 3 and 4. 	Agency action
		5. Conduct an assessment to identify stages or points in the processes for which implementing interim targets for the expected time or range of time allotted would be feasible. Establish interim targets based on the results of the assessment as appropriate.	Agency action
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes 2019-MO-B-014	09/30/2019	1. Document the role and responsibilities of the designated supervisory officer when conducting and reporting results of an internal review.	Agency action
		2. Document the training requirements for individuals assigned to perform internal reviews.	Agency action

Report title	Issuance date	Recommendation	Recommendation status
2019 Audit of the Board's Information Security Program 2019-IT-B-016	10/31/2019	1. Develop comprehensive enterprisewide guidance for the inventory of software and associated licenses throughout the Board.	Verification in progress
		2. Work with all Board divisions to ensure that an accurate and complete software and license inventory is maintained.	Verification in progress
		3. Ensure the consistent application of the Board's plan of action and milestones standard for the tracking of system- and program-level security vulnerabilities.	Verification in progress
		5. Work with the Federal Reserve System to ensure that the data loss protection replacement solution a. functions consistently across the Board's technology platforms. b. supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable.	Agency action
		6. Develop and implement a Boardwide process to incorporate the review of data loss protection logs into employee and contractor offboarding processes to identify any potential unauthorized data exfiltrations or access.	Agency action
		The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved 2020-FMIC-B-005	03/18/2020
2. Define and document which parties at the division director and governor levels will have a role in reviewing and approving enforcement actions for designated financial market utilities.	Agency action		
4. Assess the Board's core objectives in overseeing designated financial market utilities for which it is not the supervisory agency. Based on this assessment, create guidance that addresses the Board's preferred method for communicating examination findings to other supervisory agencies.	Agency action		
5. Develop a process for reconciling the Board's examination findings for designated financial market utilities for which it is not the supervisory agency with those of the other supervisory agencies and tracking the adoption of the Board's findings.	Agency action		

Report title	Issuance date	Recommendation	Recommendation status
		6. Discuss with relevant Board and Reserve Bank staff and document <ol style="list-style-type: none"> a. the various situations that could prompt emergency changes. b. the review process for emergency changes. 	Agency action
The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced 2020-SR-B-019	09/30/2020	6. Develop a structured cybersecurity training plan for cybersecurity examiners. As part of the plan, define expectations for skill sets and for continuing education, such as training related to emerging risks.	Agency action
		7. Require that relevant examiners complete cybersecurity training in a manner consistent with the plan to address recommendation 6.	Agency action
		8. Update the Board's April 2018 guidance on the Cyber Event Repository to clearly define the types of cybersecurity events that should be entered into the system.	Agency action
		9. Develop instructions and training on using the Cyber Event Repository, and issue guidance that requires central points of contact, or their designees, to complete this training.	Agency action