

# 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, 2022, 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. We recognize that some recommendations may require complex actions; therefore, our twice-yearly open recommendations reports to the Board include only recommendations that have been open for more than 12 months.

**Table 1. Status of Recommendations for 2016–2022, as of September 30, 2022**

Status	2016	2017	2018	2019	2020	2021	2022
Recommendations	40	41	57	22	43	23	14
Open	1	2	9	2	6	4	13
Closed	39	39	48	20	37	19	1
Public recommendations	30	41	37	22	43	23	12
Open	1	2	4	2	6	4 <sup>a</sup>	11 <sup>a</sup>
Closed	29	39	33	20	37	19	1
Nonpublic recommendations	10	0	20	0	0	0	2
Open	0	0	5	0	0	0	2
Closed	10	0	15	0	0	0	0

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

<sup>a</sup> 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, 2022, 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](mailto: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
<a href="#">2016 Audit of the Board's Information Security Program</a> 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.	Agency action
<a href="#">The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing</a> 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
<a href="#">2017 Audit of the Board's Information Security Program</a> 2017-IT-B-018	10/31/2017	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
<a href="#">2018 Audit of the Board's Information Security Program</a> 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
<a href="#">The Board Can Strengthen Information Technology Governance</a> 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.  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.  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  Agency action  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	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	1. Publish in an order or rule subject to the Administrative Procedure Act the internal delegations made to the Division of Reserve Bank Operations and Payment Systems for reviewing and approving advance notices of proposed change.	Agency action
		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
		6. Discuss with relevant Board and Reserve Bank staff and document a. the various situations that could prompt emergency changes. b. the review process for emergency changes.	Agency action
2020 Audit of the Board's Information Security Program 2020-IT-B-020	11/02/2020	3. Ensure that the Board's continuous monitoring processes include the security control requirements for applicable network devices.	Agency action
The Board's Implementation of Enterprise Risk Management Continues to Evolve and Can Be Enhanced 2021-IT-B-011	09/15/2021	1. Work with Board divisions to conduct an assessment of the current risk management practices and risk culture across the agency and use the results to inform the direction of the Board's enterprise risk management program.	Agency action

Report title	Issuance date	Recommendation	Recommendation status
		2. Work with the administrative governor, as appropriate, to determine an optimal governance structure and associated reporting relationships for the agency's enterprise risk management program and update the Delegations of Administrative Authority accordingly.	Agency concurrence