Report Highlights

Federal Reserve: 2026 Information Security Program Audit

Why This Matters

A strong information security program is essential for the Board of Governors of the Federal Reserve System to protect the sensitive data it uses to inform decisions that affect employment, inflation, and economic stability for 342 million Americans.

Key Results

According to federal metrics for evaluating agencies' information security programs, the Board's information security program has a maturity level of 2 out of a possible 5, meaning its program is defined but not consistently implemented, and is therefore not considered effective. We found weaknesses in several areas:

- Governance gaps, decentralized IT operations, and inconsistent policy enforcement limit comprehensive security oversight and create potential vulnerabilities.
- Outdated and incomplete policies and standards result in staff relying on institutional knowledge, which increases the risk of security vulnerabilities during personnel transitions.
- Contingency planning processes are not fully coordinated between IT groups, and contingency plans cover entire divisions instead of specific IT systems as required by federal guidelines. As a result, the Board has limited assurance that critical systems can be recovered consistently and timely during disruptions.

Further, 13 of 17 recommendations from our prior annual information security audits remain open and unimplemented.

Action Needed

We have 8 new recommendations to strengthen enterprise IT governance and oversight and to implement effective policy, standards, and processes. The Board agreed with our recommendations and outlined its planned actions to address them. We will follow up to ensure that the recommendations are fully addressed.

October 28, 2026
Audit Report
2026-IT-B-018