June 2003

FDIC INFORMATION SECURITY

Progress Made but Existing Weaknesses Place Data at Risk

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-03-630, a report to the Board of Directors, Federal Deposit Insurance Corporation

Why GAO Did This Study

Effective controls over information systems are essential to ensuring the protection of financial and personnel information and the security and reliability of bank examination data maintained by the Federal Deposit Insurance Corporation (FDIC). As part of GAO's 2002 financial statement audits of the three FDIC funds, we assessed (1) the corporation's progress in addressing computer security weaknesses found in GAO's 2001 audit, and (2) the effectiveness of FDIC's controls.

What GAO Recommends

In order to establish an effective information system control environment, in addition to fully addressing the recommendations stemming from the 2001 review, GAO recommends that the Chairman instruct the acting chief information officer to ensure that actions are completed to correct the weaknesses identified during GAO's 2002 review. In commenting on a draft of this report FDIC agreed with our recommendations. FDIC plans to address the identified weaknesses and stated that significant progress has already been made.

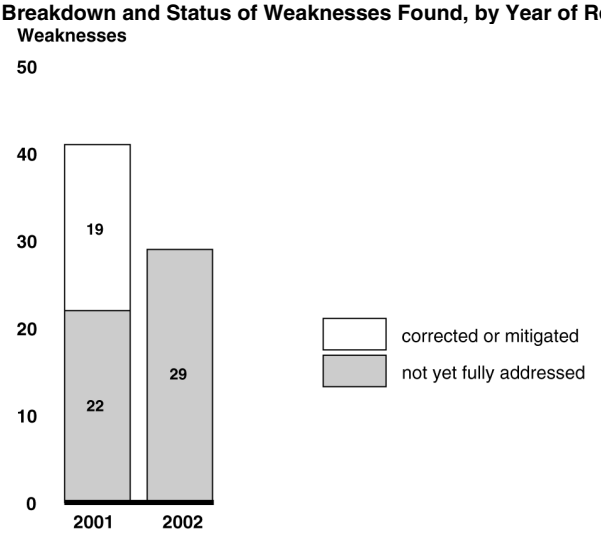
www.gao.gov/cgi-bin/getrpt?GAO-03-630.

To view the full report, including the scope and methodology, click on the link above. For more information, contact Robert Dacey at (202) 512-3317 or daceyr@gao.gov.

What GAO Found

FDIC has made progress in correcting information system controls since GAO's 2001 review. Of the 41 weaknesses identified that year, FDIC has corrected or has specific action plans to correct all of them (see figure). GAO's 2002 audit nonetheless identified 29 new computer security weaknesses. These weaknesses reduce the effectiveness of FDIC's controls to safeguard critical financial and other sensitive information.

Breakdown and Status of Weaknesses Found, by Year of Review



Source: GAO.

Based on our review, mainframe access was not sufficiently restricted, network security was inadequate, and a program to fully monitor access activities was not implemented. Additionally, weaknesses in areas including physical security, application software, and service continuity further increased the risk to FDIC's computing environment.

The primary reason for these continuing weaknesses is that FDIC has not yet completed development and implementation of a comprehensive program to manage computer security across the organization. FDIC has, among other things, established a security management structure, but still has not fully implemented a process for assessing and managing risk on a continuing basis or an ongoing program of testing and evaluating controls. The corporation's acting chief information officer has agreed to complete actions intended to address GAO's outstanding recommendations by December 31 of this year.