May 2005

INFORMATION SECURITY

Federal Deposit Insurance Corporation Needs to Sustain Progress

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-05-486, a report to the Board of Directors, Federal Deposit Insurance Corporation

Why GAO Did This Study

The Federal Deposit Insurance Corporation (FDIC) relies extensively on computerized systems to support its financial and mission-related operations. As part of GAO's audit of the calendar year 2004 financial statements for the three funds administered by FDIC, GAO assessed (1) the progress FDIC has made in correcting or mitigating information system control weaknesses identified in our audits for calendar years 2002 and 2003 and (2) the effectiveness of the corporation's information system general controls.

What GAO Recommends

To improve information system controls, GAO recommends that the FDIC Chairman direct the Chief Information Officer to implement an ongoing, comprehensive process of tests and evaluations to ensure that all key control areas supporting FDIC's financial environment are routinely reviewed and tested. In commenting on a draft of this report, FDIC agreed with our recommendations. FDIC plans to address the identified weaknesses and indicated that significant progress has already been made.

www.gao.gov/cgi-bin/getrpt?GAO-05-486.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

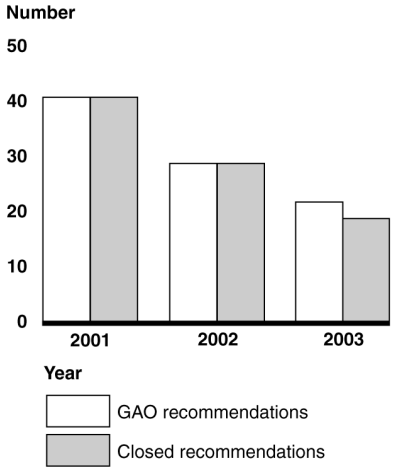
What GAO Found

FDIC has made significant progress in correcting previously reported information system control weaknesses and has taken other steps to improve information security. Of the 22 weaknesses reported in GAO's 2003 audit, FDIC corrected 19 and is taking action to resolve the 3 that remain. In addition, it corrected the one weakness still open from GAO's 2002 audits (see figure).

Although FDIC has made substantial improvements in its information system controls, GAO identified additional weaknesses that diminish FDIC's ability to effectively protect the integrity, confidentiality, and availability of its financial and sensitive information systems. These included weaknesses in electronic access controls, network security, segregation of computer functions, physical security, and application change control. Although these do not pose significant risks to FDIC's financial and sensitive systems, they warrant management's action to decrease the risk of unauthorized modification of data and programs, inappropriate disclosure of sensitive information, or disruption of critical operations.

A key reason for FDIC's weaknesses in information system controls is that it had not fully implemented a complete test and evaluation process, which is a key element of a comprehensive agency information security program with effective controls. Although FDIC has made substantial progress in implementing its information security program and has enhanced its process to test and evaluate its information system controls, it did not ensure that all key control areas supporting FDIC's financial environment are routinely reviewed and tested. These control areas included electronic access, network security, and audit logging.

FDIC Progress in Implementing GAO Recommendations



Source: GAO.