May 2004

INFORMATION SECURITY

Information System Controls at the Federal Deposit Insurance Corporation

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-04-630, 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 our calendar year 2003 financial statement audits of three FDIC Funds, GAO assessed the effectiveness of the corporation's general controls on its information systems. Our assessment included follow up on the progress that FDIC has made in correcting or mitigating computer security weaknesses identified in our audits for calendar years 2001 and 2002.

What GAO Recommends

To establish an effective information system controls environment, GAO recommends that the FDIC Chairman instruct the chief information officer, who is the corporation's key official for computer security, to correct a number of information security weaknesses, including strengthening the testing and evaluation element of its computer security management program. 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-04-630.

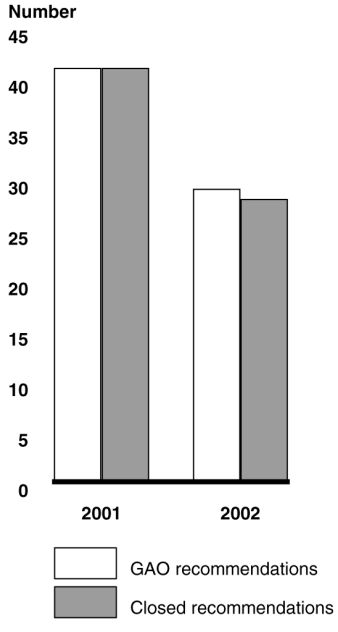
To view the full product, including the scope and methodology, click on the link above. For more information, contact Robert F. Dacey at (202) 512- 3317 or daceyr@gao.gov.

What GAO Found

FDIC has made significant progress in correcting prior year information security weaknesses. The corporation addressed almost all the computer security weaknesses we previously identified in our audits for calendar years 2001 and 2002 (see figure). Nonetheless, testing in our calendar year 2003 audit identified additional computer control weaknesses in FDIC's information systems. These weaknesses place critical FDIC financial and sensitive examination information at risk of unauthorized disclosure, disruption of operations, or loss of assets.

A key reason for FDIC's continuing weaknesses in information system controls is that it has not yet fully established a comprehensive security management program to ensure that effective controls are established and maintained and that information security receives significant management attention. The corporation only recently established a program to test and evaluate its computer control environment, and this program does not yet include adequate provisions to ensure that (1) all key computer resources supporting FDIC's financial environment are routinely reviewed and tested, (2) weaknesses detected are analyzed for systemic solutions, (3) corrective actions are independently tested, and (4) newly identified weaknesses or emerging security threats are incorporated into the test and evaluation process.

FDIC Progress in Implementing GAO Recommendations



Source: GAO.