

Why GAO Did This Study

The Internal Revenue Service (IRS) has a demanding responsibility in collecting taxes, processing tax returns, and enforcing the nation's tax laws. It relies extensively on computerized systems to support its financial and mission-related operations and on information security controls to protect the financial and sensitive taxpayer information that resides on those systems.

As part of its audit of IRS's fiscal years 2012 and 2011 financial statements, GAO assessed whether controls over key financial and tax-processing systems are effective in ensuring the confidentiality, integrity, and availability of financial and sensitive taxpayer information. To do this, GAO examined IRS information security policies, plans, and procedures; tested controls over key financial applications; and interviewed key agency officials at eight sites.

What GAO Recommends

GAO recommends that IRS take four actions to more effectively implement portions of its information security program. In a separate report with limited distribution, GAO is recommending that IRS take 30 specific actions to address newly identified control weaknesses. In commenting on a draft of this report, IRS agreed to develop a detailed corrective action plan to address each recommendation.

INFORMATION SECURITY

IRS Has Improved Controls but Needs to Resolve Weaknesses

What GAO Found

IRS continued to make progress in addressing information security control weaknesses, improving its internal control over financial reporting. During fiscal year 2012, IRS management devoted attention and resources to addressing information security controls, and resolved a significant number of the information security control deficiencies that GAO previously reported. Notable among these efforts were the (1) formation of cross-functional working groups tasked with the identification and remediation of specific at-risk control areas, (2) improvement in controls over the encryption of data transferred between accounting systems, and (3) upgrades to critical network devices on the agency's internal network system. However, serious weaknesses remain that could affect the confidentiality, integrity, and availability of financial and sensitive taxpayer data. For example, the agency had not always (1) implemented effective controls for identifying and authenticating users, such as enforcing password complexity on certain servers; (2) appropriately restricted access to its mainframe environment; (3) effectively monitored the mainframe environment; or (4) ensured that current patches had been installed on systems to protect against known vulnerabilities.

An underlying reason for these weaknesses is that IRS has not effectively implemented portions of its information security program. The agency has established a comprehensive framework for the program, and continued to make strides with various initiatives designed to improve its controls; however, certain components of the program did not always function as intended. For example, IRS's testing procedures over a financial reporting system that GAO reviewed did not always determine whether required controls were operating effectively and consequently, GAO identified control weaknesses that had not been detected by IRS. In addition, the agency had not updated an important policy concerning security standards for IRS's main tax processing environment to include current software versions and control capabilities. Further, although IRS indicated that it had addressed 58 of the previous information system security-related recommendations GAO made, 13 (about 22 percent) of the 58 had actually not yet been fully resolved. Continued and consistent management commitment and attention to an effective information security program will be essential to the maintenance of, and continued improvements in, its information system controls. Until IRS takes additional steps to (1) more effectively implement its testing and monitoring capabilities, (2) ensure that policies and procedures are updated, and (3) address unresolved and newly identified control deficiencies, its financial and taxpayer data will remain vulnerable to inappropriate use, modification, or disclosure, possibly without being detected. These deficiencies, along with shortcomings in the information security program, were the basis of GAO's determination that IRS had a significant deficiency in its internal control over financial reporting systems for fiscal year 2012.