



Highlights of [GAO-12-393](#), a report to the Commissioner of Internal Revenue

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 financial and sensitive taxpayer information that resides on those systems.

As part of its audit of IRS's fiscal years 2011 and 2010 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 seven sites.

What GAO Recommends

GAO recommends that IRS take 6 actions to fully implement key components of its comprehensive information security program. In a separate report with limited distribution, GAO is recommending that IRS take 23 specific actions to correct 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.

View [GAO-12-393](#). For more information, contact Nancy R. Kingsbury at (202) 512-2700 or kingsburyn@gao.gov or Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

March 2012

INFORMATION SECURITY

IRS Needs to Further Enhance Internal Control over Financial Reporting and Taxpayer Data

What GAO Found

IRS implemented numerous controls and procedures intended to protect key financial and tax-processing systems; nevertheless, control weaknesses in these systems continue to jeopardize the confidentiality, integrity, and availability of the financial and sensitive taxpayer information processed by IRS's systems. Specifically, the agency continues to face challenges in controlling access to its information resources. For example, it had not always (1) implemented controls for identifying and authenticating users, such as requiring users to set new passwords after a prescribed period of time; (2) appropriately restricted access to certain servers; (3) ensured that sensitive data were encrypted when transmitted; (4) audited and monitored systems to ensure that unauthorized activities would be detected; or (5) ensured management validation of access to restricted areas. In addition, unpatched and outdated software exposed IRS to known vulnerabilities, and the agency had not enforced backup procedures for a key system.

An underlying reason for these weaknesses is that IRS has not fully implemented a comprehensive information security program. IRS has established a comprehensive framework for such a program, and has made strides to address control deficiencies—such as establishing working groups to identify and remediate specific at-risk control areas; however, it has not fully implemented all key components of its program. For example, IRS's security testing and monitoring continued to not detect many of the vulnerabilities GAO identified during this audit. IRS also did not promptly correct known vulnerabilities. For example, the agency indicated that 76 of the 105 previously reported weaknesses open at the end of GAO's prior year audit had not yet been corrected. In addition, IRS did not always validate that its actions to resolve known weaknesses were effectively implemented. Although IRS had a process in place for verifying whether each weakness had been corrected, this process was not always working as intended. Of the 29 weaknesses IRS indicated were corrected, GAO determined that 13 (about 45 percent) had not yet been fully addressed.

Considered collectively, these deficiencies, both new and unresolved from previous GAO audits, along with a lack of fully effective compensating and mitigating controls, impair IRS's ability to ensure that its financial and taxpayer information is secure from internal threats. This reduces IRS's assurance that its financial statements and other financial information are fairly presented or reliable and that sensitive IRS and taxpayer information is being sufficiently safeguarded from unauthorized disclosure or modification. These deficiencies are the basis of GAO's determination that IRS had a material weakness in internal control over financial reporting related to information security in fiscal year 2011.