

Federal Information System Controls Audit Manual (FISCAM)

GAO-09-232G February 2, 2009
[Full Report \(PDF, 601 pages\)](#) [Accessible Text](#)

Summary

FISCAM presents a methodology for performing information system (IS) control audits of federal and other governmental entities in accordance with professional standards. This version supersedes the prior version, Federal Information System Controls Audit Manual: Volume I Financial Statement Audits, AIMD-12.19.6, January 1, 2001. The FISCAM is designed to be used primarily on financial and performance audits and attestation engagements performed in accordance with GAGAS, as presented in Government Auditing Standards (also know as the "Yellow Book"). The FISCAM is consistent with the GAO/PCIE Financial Audit Manual (FAM). Also, FISCAM control activities are consistent with NIST Special Publication 800-53 and all SP800-53 controls have been mapped to the FISCAM. The FISCAM, which is consistent with NIST and other criteria, is organized to facilitate effective and efficient IS control audits. Specifically, the methodology in the FISCAM incorporates the following: (1) A top-down, risk-based approach that considers materiality and significance in determining effective and efficient audit procedures; (2) Evaluation of entitywide controls and their effect on audit risk; (3) Evaluation of general controls and their pervasive impact on business process application controls; (4) Evaluation of security management at all levels (entitywide, system, and business process application levels); (5) A control hierarchy (control categories, critical elements, and control activities) to assist in evaluating the significance of identified IS control weaknesses; (6) Groupings of control categories consistent with the nature of the risk; and (7) Experience gained in GAO's performance and review of IS control audits, including field testing the concepts in this revised FISCAM.

Related Searches

Related terms:

- [Auditing procedures](#)
- [Auditing standards](#)
- [Computer security](#)
- [Data integrity](#)
- [Federal agency accounting systems](#)
- [Financial statement audits](#)
- [Information management](#)
- [Information security](#)
- [Information security management](#)
- [Information security regulations](#)
- [Information systems](#)
- [Information technology](#)
- [Internal controls](#)
- [Risk management](#)
- [Software](#)
- [Software verification and validation](#)
- [Standards evaluation](#)
- [Strategic planning](#)
- [Systems analysis](#)
- [Systems evaluation](#)
- [Systems integration](#)
- [Systems management](#)
- [Systems monitoring](#)