GAO invites comments on the proposed changes to the *Federal Information System Controls Audit Manual* (FISCAM) draft from federal, state, and local government officials; managers and auditors at all levels of government; professional organizations; public interest groups; and other interested parties. We encourage you to respond to questions from enclosure II of the FISCAM 2023 exposure draft and comment on any additional issues that you note.

Please send your comments to [FISCAM@gao.gov](mailto:FISCAM@gao.gov) no later than **October 18, 2023**. For more information, contact Dawn B. Simpson at (202) 512-3406 or [FISCAM@gao.gov](mailto:FISCAM@gao.gov).

Date: Click or tap to enter a date.

Respondent Name: Click or tap here to enter text.

Organization Name: Click or tap here to enter text.

Organization Type: Choose an item.

Please provide comments for the following specific questions from Enclosure II. In your response, please reference specific paragraphs, if applicable. If you do not have a comment for a specific question, please leave the response box blank.

1. Please comment on the clarity and appropriateness of the auditor requirements and application guidance for
   1. identifying relevant information system (IS) control objectives for each area of audit interest that are in section 240 and section 270;

Click or tap here to enter text.

* 1. selecting IS control activities (or a combination of IS control activities) that are likely to achieve the relevant control objectives and are most efficient for testing in section 320; and

Click or tap here to enter text.

* 1. determining whether sufficient, appropriate evidence for the design, implementation, and operating effectiveness of IS controls has been obtained to the extent necessary to support the achievement of the engagement objectives in section 340.

Click or tap here to enter text.

1. Please comment on the following:
   1. the usefulness of the FISCAM Assessment Completion Checklist in helping auditors determine whether they have followed FISCAM requirements and

Click or tap here to enter text.

* 1. any enhancements to improve it.

Click or tap here to enter text.

1. Please comment on how changes to guidance for assessing IS controls that external entities, including service organizations, perform on behalf of the entity are likely to affect the auditor's ability to assess IS controls that external entities perform.

Click or tap here to enter text.

1. Please comment on where the use of graphics, tools, or templates may provide clarity.

Click or tap here to enter text.

**Comments for FISCAM Section 100 Introduction**

Please provide comments for Section 100 by subsection topics as noted. In your response, please reference specific paragraphs, if applicable. For topics not addressed by subsections, please include in general comments (Item No. 18). If you do not have a comment for a specific topic, please leave the response box blank.

1. Section 110 Purpose

Click or tap here to enter text.

1. Section 110 Applicability

Click or tap here to enter text.

1. Section 120 Control Types

Click or tap here to enter text.

1. Section 120 Control Objectives

Click or tap here to enter text.

1. Section 120 Implementation Levels

Click or tap here to enter text.

1. Section 130 Organization and Content

Click or tap here to enter text.

1. Section 130 Planning Phase Summary

Click or tap here to enter text.

1. Section 130 Testing Phase Summary

Click or tap here to enter text.

1. Section 130 Reporting Phase Summary

Click or tap here to enter text.

1. Section 130 Other Information

Click or tap here to enter text.

1. Section 140 Auditing Standards

Click or tap here to enter text.

1. Section 140 Auditor Responsibility

Click or tap here to enter text.

1. Section 150 Criteria – Internal Control Standards (Green Book)

Click or tap here to enter text.

1. Section 150 Criteria – Office of Management and Budget Information and Guidance

Click or tap here to enter text.

1. Section 150 Criteria – NIST Standards and Guidelines

Click or tap here to enter text.

1. Section 150 Criteria – Department of Homeland Security Directives and Defense Information Systems Agency Security Technical Implementation Guides

Click or tap here to enter text.

1. Section 160 Overview of the FISCAM Framework

Click or tap here to enter text.

1. Section 100 General Comments

Click or tap here to enter text.

**Comments for FISCAM Section 200 Planning Phase**

Please provide comments for Section 200 by subsection topics as noted. In your response, please reference specific paragraphs, if applicable. For topics not addressed by subsections, please include in general comments (Item No. 21). If you do not have a comment for a specific topic, please leave the response box blank.

1. Section 210 Planning – Overview

Click or tap here to enter text.

1. Section 220 Planning – Competence

Click or tap here to enter text.

1. Section 220 Planning – Communication of Engagement Information

Click or tap here to enter text.

1. Section 230 Planning – Understand the Entity’s Operations

Click or tap here to enter text.

1. Section 230 Planning – Identify and Understand Significant Business Processes

Click or tap here to enter text.

1. Section 240 Planning – Identify Areas of Audit Interest

Click or tap here to enter text.

1. Section 240 Planning – Understand Business Process Controls

Click or tap here to enter text.

1. Section 250 Planning – Understand the Entity’s Information Security Management Program

Click or tap here to enter text.

1. Section 250 Planning – Understand the Entity’s Information Security Management Program Using the FISCAM Framework

Click or tap here to enter text.

1. Section 260 Planning – Identify Inherent Risk Factors

Click or tap here to enter text.

1. Section 260 Planning – Identify Control Risk Factors

Click or tap here to enter text.

1. Section 260 Planning – Identify Fraud Risk Factors

Click or tap here to enter text.

1. Section 260 Planning – Results of Previous Engagements

Click or tap here to enter text.

1. Section 260 Planning – Assess IS Risk on a Preliminary Basis

Click or tap here to enter text.

1. Section 270 Planning – Identify Relevant General Control Objectives Using the FISCAM Framework

Click or tap here to enter text.

1. Section 270 Planning – Determine Likelihood of Effective General Controls Using the FISCAM Framework

Click or tap here to enter text.

1. Section 280 Planning Documentation – Risk Assessment

Click or tap here to enter text.

1. Section 280 Planning Documentation – Audit Plan

Click or tap here to enter text.

1. Section 280 Planning Documentation – Planning Memo

Click or tap here to enter text.

1. Section 280 Planning Documentation – Subordinate Test Plans

Click or tap here to enter text.

1. Section 200 General Comments – Planning Phase

Click or tap here to enter text.

**Comments for FISCAM Section 300 Testing Phase**

Please provide comments for Section 300 by subsection topics as noted. In your response, please reference specific paragraphs, if applicable. For topics not addressed by subsections, please include in general comments (Item No. 17). If you do not have a comment for a specific topic, please leave the response box blank.

1. Section 310 Testing – Overview

Click or tap here to enter text.

1. Section 320 Testing – Select User, Application, and General Control Activities

Click or tap here to enter text.

1. Section 330 Testing – Nature of IS Control Tests

Click or tap here to enter text.

1. Section 330 Testing – Extent of IS Control Tests

Click or tap here to enter text.

1. Section 330 Testing – Timing of IS Control Tests

Click or tap here to enter text.

1. Section 330 Testing – Automated Audit Tools

Click or tap here to enter text.

1. Section 330 Testing – Considerations for Testing IS Controls That Service Organizations Perform

Click or tap here to enter text.

1. Section 340 Testing – Perform IS Control Tests

Click or tap here to enter text.

1. Section 340 Testing – Determine Whether Relevant IS Control Objectives Are Achieved

Click or tap here to enter text.

1. Section 340 Testing – Evaluate the Significance of IS Control Deficiencies

Click or tap here to enter text.

1. Section 340 Testing – Assess Sufficiency and Appropriateness of Evidence and Level of Audit Risk

Click or tap here to enter text.

1. Section 350 Testing – Audit Plan

Click or tap here to enter text.

1. Section 350 Testing – Results Memo

Click or tap here to enter text.

1. Section 350 Testing – Subordinate Test Plans

Click or tap here to enter text.

1. Section 350 Testing – Sampling Plans

Click or tap here to enter text.

1. Section 350 Testing – Technical Reviews

Click or tap here to enter text.

1. Section 300 General Comments – Testing Phase

Click or tap here to enter text.

**Comments for FISCAM Section 400 Reporting Phase**

Please provide comments for Section 400 by subsection topics as noted. In your response, please reference specific paragraphs, if applicable. For topics not addressed by subsections, please include in general comments (Item No. 5). If you do not have a comment for a specific topic, please leave the response box blank.

1. Section 410 Reporting – Overview

Click or tap here to enter text.

1. Section 420 Reporting – Determine Compliance with FISCAM

Click or tap here to enter text.

1. Section 430 Reporting – Objectives, Scope, and Methodology

Click or tap here to enter text.

1. Section 430 Reporting – Findings, Conclusions, and Recommendations

Click or tap here to enter text.

1. Section 430 Reporting – Presentation of Findings, Conclusions, and Recommendations

Click or tap here to enter text.

1. Section 430 Reporting – Reporting Confidential or Sensitive Information

Click or tap here to enter text.

1. Section 440 Reporting – Departures from FISCAM

Click or tap here to enter text.

1. Section 400 General Comments – Reporting Phase

Click or tap here to enter text.

**Comments for FISCAM Section 500 (Appendixes)**

Please provide comments for Section 500 by appendix. For appendix 500A, please reference specific glossary terms, if applicable, in your response. For appendix 500B, please reference specific index numbers from the tables (e.g., SM.01.02.03), if applicable, in your response. For appendix 500C, please reference specific question numbers, if applicable, in your response. If you do not have a comment for a specific topic, please leave the response box blank.

1. Appendix 500A General Comments – Glossary

Click or tap here to enter text.

1. Appendix 500B General Comments – FISCAM Framework

Click or tap here to enter text.

1. Appendix 500B Table 8, FISCAM Framework for Business Process Controls

Click or tap here to enter text.

1. Appendix 500B Table 9, FISCAM Framework for Security Management

Click or tap here to enter text.

1. Appendix 500B Table 10, FISCAM Framework for Access Controls

Click or tap here to enter text.

1. Appendix 500B Table 11, FISCAM Framework for Segregation of Duties

Click or tap here to enter text.

1. Appendix 500B Table 12, FISCAM Framework for Configuration Management

Click or tap here to enter text.

1. Appendix 500B Table 13, FISCAM Framework for Contingency Planning

Click or tap here to enter text.

1. Appendix 500C General Comments – FISCAM Assessment Completion Checklist

Click or tap here to enter text.