EY
Building a better
working world

Ernst & Young LLP
One Manhattan West
New York, NY 10001-8604

Tel: +1 212 773 3000
ey.com

Ms. Dawn B. Simpson
Director
Government Accountability Office
441 G Street, NW
Washington, D.C. 20548

18 October 2023

VIA E-MAIL: FISCAM@gao.gov

Federal Information System Controls Audit Manual (FISCAM)
2023 Exposure Draft

Dear Ms. Simpson:

Ernst & Young LLP is pleased to submit our comments to the U.S. Government Accountability Office (GAO) in response to its request for comment on the Federal Information System Controls Audit Manual (FISCAM) 2023 exposure draft.

We support the GAO's efforts to update the FISCAM to reflect changes in relevant auditing standards, guidance, control criteria and technology. We have provided our comments and responses to certain questions in the GAO-provided fillable form attached below.

*   *   *   *   *

We would be pleased to discuss our comments at your convenience.

Very truly yours,

Ernst + Young LLP

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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 no later than **October 18, 2023**. For more information, contact Dawn B. Simpson at (202) 512-3406 or FISCAM@gao.gov.

Date: October 18, 2023

Respondent Name: This item is left blank

Organization Name: Ernst & Young LLP

Organization Type: Accounting Firm

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

    a. identifying relevant information system (IS) control objectives for each area of audit interest that are in section 240 and section 270;

    Comment 01-Section 270: There are multiple areas where the FAM is referenced in the updated FISCAM. We recommend adding a statement in the FISCAM indicating that for areas related to the financial statement audits where the auditor uses judgment to identify conflicts between the FAM and FISCAM, the auditor should follow the FAM, rather than FISCAM.

    In addition, we noted that the FISCAM lacks a true reference of workflow between the FAM and FISCAM documents. We recommend implementing a table or graphic to help demonstrate this workflow from a FISCAM perspective, which should be similar to the graphic in the FAM (FAM 295 J, figure 1).

b. 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

Comment 01-Section 320: We recommend addressing the relationship between the identified risks in connection with the audit interest areas and the selection of the control activities for testing. The inclusion of identified risks would provide the auditor with a framework for selecting each of the controls to address the risks relating to the audit interest areas.

For example, one of the risks of a material misstatement when conducting a financial statement audit is having unauthorized users perform inappropriate transactions that impact the financial reporting data. Auditors generally select access provisioning controls to test to mitigate such risk.

c. 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.

2. Please comment on the following:

a. the usefulness of the FISCAM Assessment Completion Checklist in helping auditors determine whether they have followed FISCAM requirements and

Comment 01-Section 500C: While we understand the purpose and content of APPENDIX 500C, the FISCAM Assessment Complement Checklist (the Checklist), we recommend clarifying in FISCAM that the Checklist would serve as a guide for auditors when using FISCAM and would not be required documentation. This recommendation aligns with the purpose of FISCAM as a “methodology for assessing the design, implementation, and operating effectiveness of information system controls.” (FISCAM 110.01) The Checklist implies that compliance with FISCAM would be required and that all GAGAS Information Systems (IS) assessments would have to comply with FISCAM.

b. any enhancements to improve it.

Click or tap here to enter text.

3. 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.

Comment 01-Section 330: The proposed changes would clarify the auditor’s process of assessing controls provided by the service organization(s) used by the entity, which include SOC report evaluation and direct testing as needed. The proposed changes would enhance the auditor’s approach in testing the controls in this category.

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

Comment 01: We recommend including graphics to illustrate the overview for types of IS controls and control objectives (section 120) and information technology (IT) environment components that would help auditors to further understand the objectives when testing the controls within each component at both the business process and system control levels. In addition, we recommend including graphics to illustrate the new FISCAM Phases and key talking points for each section to provide auditors with more clarity.

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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.

2. Section 110 Applicability

   Click or tap here to enter text.

3. Section 120 Control Types

   Click or tap here to enter text.

4. Section 120 Control Objectives

   Click or tap here to enter text.

5. Section 120 Implementation Levels

   Click or tap here to enter text.

6. Section 130 Organization and Content

   Click or tap here to enter text.

7. Section 130 Planning Phase Summary

   Click or tap here to enter text.

8. Section 130 Testing Phase Summary

   Click or tap here to enter text.

9. Section 130 Reporting Phase Summary

Click or tap here to enter text.

10. Section 130 Other Information

    Click or tap here to enter text.

11. Section 140 Auditing Standards

    Click or tap here to enter text.

12. Section 140 Auditor Responsibility

    Click or tap here to enter text.

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

    Click or tap here to enter text.

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

    Click or tap here to enter text.

15. Section 150 Criteria – NIST Standards and Guidelines

    Click or tap here to enter text.

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

    Click or tap here to enter text.

17. Section 160 Overview of the FISCAM Framework

    Click or tap here to enter text.

18. Section 100 General Comments

    Click or tap here to enter text.

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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.

2. Section 220 Planning – Competence

   Click or tap here to enter text.

3. Section 220 Planning – Communication of Engagement Information

   Click or tap here to enter text.

4. Section 230 Planning – Understand the Entity's Operations

   Click or tap here to enter text.

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

   Comment 01-Section 230: In sub-section .08 of Section 230, FISCAM states that the auditor should perform walk-throughs of the significant business processes to identify areas of audit interest, specifically the use of IS, information system components and information system resources for the business processes. Technology continues to evolve, and more complex automation and application functionality are being introduced to business processes. This automation may not always be evident in walk-throughs. Therefore, we recommend indicating explicitly that the auditor would be expected to understand automation in the significant business processes, including the technology that enables it.

   We recommend that supporting IT tools be included as a listed IS environment element that the auditor should examine when evaluating which IS support each significant business process. Examples of supporting technology include (1) robotic process automation (RPA) applications that support information system processes, (2) desktop software plugin technology, like Hyperion SmartView for Microsoft Excel, (3) ticketing tools with workflows used to capture approvals for changes or access before they are administered (e.g., JIRA and ServiceNow) and (4) software used to monitor the ongoing appropriateness of application/database/operating system security settings.

Comment 02-Section 230: We recommend stating that one of the objectives of walk-throughs is to identify areas of audit interest, rather that stating that walkthroughs are (solely) used for that purpose. Additional objectives include but may not be limited to understanding business process, control design and IT process flows. We also recommend incorporating walk-through definitions and guidance from FAM 320.

6. Section 240 Planning – Identify Areas of Audit Interest

   Click or tap here to enter text.

7. Section 240 Planning – Understand Business Process Controls

   Click or tap here to enter text.

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

   Click or tap here to enter text.

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

   Click or tap here to enter text.

10. Section 260 Planning – Identify Inherent Risk Factors

    Click or tap here to enter text.

11. Section 260 Planning – Identify Control Risk Factors

    Click or tap here to enter text.

12. Section 260 Planning – Identify Fraud Risk Factors

    Comment 01-Section 260: We recommend that GAO clarify the phrase in the bullet in Section 260 from “including any specific fraud risks or suspected fraud associated with the information technology that the entity employs” to “including any specific fraud risks or suspected fraud associated with the information technology the entity uses.”

13. Section 260 Planning – Results of Previous Engagements

Click or tap here to enter text.

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

    Click or tap here to enter text.

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

    Click or tap here to enter text.

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

    See our response in section 1a above.

17. Section 280 Planning Documentation – Risk Assessment

    Click or tap here to enter text.

18. Section 280 Planning Documentation – Audit Plan

    Click or tap here to enter text.

19. Section 280 Planning Documentation – Planning Memo

    Click or tap here to enter text.

20. Section 280 Planning Documentation – Subordinate Test Plans

    Click or tap here to enter text.

21. Section 200 General Comments – Planning Phase

    Click or tap here to enter text.

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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.

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

   See our response in section 1b above.

3. Section 330 Testing – Nature of IS Control Tests

   Click or tap here to enter text.

4. Section 330 Testing – Extent of IS Control Tests

   Comment 01-Section 330: GAGAS contains general requirements for audit methodologies and refers to detailed guidance on the sample methodology for each type of engagement. We recommend enhancing the description to refer the auditors back to GAGAS for authoritative guidance relating to sampling, because we believe this would help prevent inconsistencies and confusion if GAGAS is updated.

5. Section 330 Testing – Timing of IS Control Tests

   Comment 01-Section 330: We recommend enhancing the specificity of the timing guidance to mitigate ambiguity and minimize the risk of varied interpretations during reviews. Additionally, we recommend including additional testing procedures and guidance to make sure comprehensive evaluation of the effectiveness of IS controls is covered for the full period under evaluation.

6. Section 330 Testing – Automated Audit Tools

   Comment 01-Section 330: We recommend a comprehensive review of references throughout the document to improve the accuracy of the exposure draft. For example, we believe the reference in Section 330.38 to Section 330.29 is incorrect and should be changed to Section 330.30.

   Comment 02–Section 330: Section 330.30 discusses full population testing and defines a deviation as a single failure. While this definition of deviation aligns with entirely automated actions, it may not accurately capture scenarios involving human involvement, where errors are likely. We believe the concept of full population testing should be clarified to make sure it is interpreted accurately and consistently. For example, full population testing could be considered substantive testing rather than controls testing.

Lastly, the guidance in Section 330.32 doesn't clearly address the analysis of completeness and accuracy procedures for data collection sources, particularly within the IS domain. We recommend clarifying these aspects to make sure the control framework is implemented in a comprehensive and effective manner. Refer to EY's comment letter on the PCAOB's proposal on the auditor's use of technology assisted analysis for further discussion (Link: https://assets.pcaobus.org/pcaob-dev/docs/default-source/rulemaking/docket-052/14_ey.pdf?sfvrsn=ecc39dba_4).

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

   See our response in section 3 above.

8. Section 340 Testing – Perform IS Control Tests

   Click or tap here to enter text.

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

   Click or tap here to enter text.

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

    Click or tap here to enter text.

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

    Click or tap here to enter text.

12. Section 350 Testing – Audit Plan

    Click or tap here to enter text.

13. Section 350 Testing – Results Memo

Click or tap here to enter text.

14. Section 350 Testing – Subordinate Test Plans

Click or tap here to enter text.

15. Section 350 Testing – Sampling Plans

Click or tap here to enter text.

16. Section 350 Testing – Technical Reviews

Click or tap here to enter text.

17. Section 300 General Comments – Testing Phase

Click or tap here to enter text.

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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.

2. Section 420 Reporting – Determine Compliance with FISCAM

   Click or tap here to enter text.

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

   Click or tap here to enter text.

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

   Click or tap here to enter text.

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

   Click or tap here to enter text.

6. Section 430 Reporting – Reporting Confidential or Sensitive Information

   Click or tap here to enter text.

7. Section 440 Reporting – Departures from FISCAM

   Click or tap here to enter text.

8. Section 400 General Comments – Reporting Phase

   Click or tap here to enter text.

Request for Public Comments

Federal Information System Controls Audit Manual

2023 Exposure Draft

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

   Comment 01-Appendix 500A: We recommend performing a comprehensive review of significant terminologies used throughout the proposal, including in the glossary section, to make sure a complete list of definitions for the significant topics is included in the glossary section. We believe this would enhance the clarity of the proposal's subject matters. For example, there are no definitions for CUECs and Simple Random Selection, which are terms mentioned in previous sections.

2. Appendix 500B General Comments – FISCAM Framework

   Comment 01-Appendix 500B: We recommend limiting the use of the phrase "when practical" in the control testing procedure guidance, because "when practical" is subjective and can be incorrectly interpreted.

   Comment 02-Appendix 500B: The exposure draft references and defines completeness and accuracy. However, it doesn't specifically address the depth and rigor that may be required for an auditor to reach the level of understanding necessary. We recommend adding language stating that "information provided by the entity procedures could include but may not be limited to" and adding associated guidance for IT-related populations and the different procedures that may be required to validate the completeness and accuracy of a population.

   We believe it is important to recognize that different types of procedures may be necessary, depending on the IPE, to include management's procedures for validating the completeness and accuracy of populations used in its own controls. With continuous technology changes, the auditor will encounter more complexity for the validation of completeness and accuracy (e.g., how does an auditor validate the completeness and accuracy of the data related to a population of changes generated from a ticketing tool? Is the retrieval tool extracting complete and accurate data?).

   Additionally, it is important for the auditor to assess management's own procedures over completeness and accuracy and their evolution as technology changes (e.g., from completeness and accuracy over a point-in-time user listing used for a user access review evolving to completeness and accuracy over a tool or module for rolling user access reviews).

   Comment 03-Appendix 500B: While the related controls listed for each control activity

would be clear and detailed, we recommend reviewing all the related control mappings to make sure they are consistent and accurate. The following is a non-exhaustive list of control mapping issues we have identified:
1) While CP.01.04.02 states that CP.03.01.01 is a related control, CP.03.01.01 does not exist in the current proposal draft.
2) While CM.02.01.01 and CM.02.02.01 appear to be related controls because they reference the same controls and relate to the same NIST criteria, they do not reference each other.
3) While CM.01.01.03, CM.01.04.01 and CM.02.03.01 all relate to baselines and agree to the same NIST criteria, only CM.01.04.01 and CM.02.03.01 list each other as related controls, and CM.01.01.03 is not mentioned by either control. Additionally, CM.01.01.03 lists a different control (CM.01.01.02) as a related control.

Comment 04-Appendix 500B: We recommend further clarifying the definition of “sensitive” in the “illustrative control activities” description in the context of testing controls. The definition on page 500A-31 implies either confidentiality, more privacy or a cyber-focused perspective to IT control owners (especially in DoD or IC spaces) as opposed to process relevancy at the business process level (especially in DoD or IC spaces). We recommend using an alternative term to reach the desired control objective, such as “relevant” or “financially significant,” as used in BP.04.06.02 and BP.06.03.07.

Additionally, we recommend reevaluating the use of “sensitive” throughout the exposure draft and making sure there is guidance on the interpretation of “sensitive” for each context in which it is used. For example, “sensitive” could be interpreted as a security classification of data in a data management context. “Sensitive” in business process transactions could mean high risk transactions that could have significant impact on financial reporting data.

Comment 05-Appendix 500B: We recommend expanding the examples of relevant risks relating to the controls listed in the control tables (8-13). This would allow auditors to understand the related controls that address those risks. We believe that providing additional examples of risks relating to financial audits would benefit the auditor.

Comment 06-Appendix 500B: We recommend adding Rev 5 into the NIST reference in the “relevant criteria” column to notate the reference of Rev.5 to prevent confusion if NIST SP 800-53 is updated before FISCAM is.

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

Comment 01-Appendix 500B table 8: While the illustrative procedures for business process controls provide insights on the procedures the auditor can leverage to address the controls selected for testing, we recommend revising the language to make it more concise, focus on fundamental testing procedures (inquiry, inspection, observation and re-performance) as appropriate and give auditors more flexibility in designing the procedures that appropriately address the control-related risks.

Comment 02-Appendix 500B table 8 - BP.04.04: We recommend reevaluating whether to include privacy controls (such as PII) and test them as part of the business process controls. We believe it would be beneficial to move the privacy controls in BP to the Security Management control domain, so they are addressed at the system level instead of at each business process level.

Comment 03-Appendix 500B table 8: The proposed standard states “BP.04.03.02 Business processes are standardized and automated when practicable.” We recommend removing “automated” from the wording of this control because the risk of not having a business process automated may impact the control objectives from the perspectives of data integrity and validity.

Additionally, while current technology trends indicate a continued rise in automation, we believe auditors should consider this aspect in the BP domain, and we are aware that many federal entities still have system limitations that prevent them from achieving a certain level of automation. If GAO decides to not to remove “automated” from the wording of the control, we recommend that it provide additional guidance on testing systems with limitations that gives the auditor flexibility in designing the testing approach for these controls. We have the same recommendations with respect to BP.04.03.03.

Comment 04-Appendix 500B table 8 - BP.04.07.03: We recommend changing the phrase "employs integrity verification tools" to "employs verification processes to detect unauthorized changes" because the implementation of such tools may not be feasible in certain instances. If GAO decides not to change the wording as we suggest, we recommend that it provide additional guidance on testing systems with limitations to give the auditor flexibility in designing the testing approach for these controls.

Comment 05-Appendix 500B table 8: Given the significant automation in business process controls, we recommend adding additional emphasis on the testing approach for the auditors to gain a detailed understanding of the design of the automation that may include the inspection of program codes (e.g., source codes if feasible, scripts and job schedules involving the execution of the controls). The emphasis of program code inspection in the testing approach would help the auditor better understand the different processing alternatives that should be tested. As business processes become more complex, performing an observation of one of the illustrative audit procedures for business controls may not always be sufficient.

Comment 06-Appendix 500B table 8: We recommend grouping some of the sub-control activities to provide a more seamless testing approach for auditors when planning and testing. For example, BP.02.01.03, BP.02.01.04, BP.02.01.05 and BP.02.01.06 are related to the generation, review, reconciliation and correction of errors resulting from data processing. Further, this observation also applies to BP.05.04.01, BP.05.04.02, BP.05.04.03, BP.05.04.05 and BP.05.04.06, which provide reasonable assurance that interface processing is monitored and actions are taken once anomalies are identified.

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

Click or tap here to enter text.

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

   Comments 01-Appendix 500B table 10 - AC.02.03.01: In instances where access is not provisioned or reviewed at the lowest level (i.e., permission/authorization), we recommend considering the necessity of conducting overall roles-to-permission reviews, at least annually. This control is designed to make sure roles and permissions/authorizations matrices are accurate while also prompting the auditor to consider whether implementing such reviews universally for significant IS systems would be an appropriate and beneficial step.

   Question 02-Appendix 500B table 10: AC.02.03.02 and AC.02.03.08 as written in the exposure draft appear to be the same. We recommend rewriting one of these items to address a different risk. For example, we suggest adding a control to focus on the review of user roles or changes to access levels within the IT systems to verify that the roles and permissions matrices are accurate and up to date.

   Comments 03-Appendix 500B table 10 - AC.02.03.01, AC.02.03.08, AC.04.01.03: We recommend evaluating the consistency of completeness and accuracy procedures within management review controls. For example, controls AC.02.03.01 and AC.04.01.03 do not identify completeness and accuracy procedures, but AC.02.03.08 does.

   Additionally, to reinforce management responsibility, we suggest incorporating testing of management-implemented completeness and accuracy controls. We also recommend considering the competence and authority of the reviewers conducting the reviews, which we believe are vital for making sure the appropriateness of user access is evaluated accurately.

   Comments 04-Appendix 500B table 10 - AC.02.03 control area: As the IT landscape evolves with increased reliance on automation, we recommend examining the risks associated with automated processes within IT general controls. Specifically, attention should be given to automation's impact on critical functions, such as access provisioning, modifications, terminations and user access reviews.

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

   Comment 01-Appendix 500B table 11: Since Segregation of Duties is listed as its own control domain within the IT general controls, we suggest expanding the content in the exposure draft to include the segregation of duties considerations in business process, rather than a least privilege consideration, which is already covered within the access controls domain.

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

   Comment 01-Appendix 500B table 12 - CM.02.02 & CM.02.04: We recommend including both the logging and monitoring of emergency/shared accounts within the change management process. In addition, we recommend including the consideration of the competency and authority of the reviewers performing the monitoring to ensure an effective evaluation of activities performed by the accounts. We believe these changes are essential due to the heightened security risks associated with such accounts. Robust monitoring can effectively detect and mitigate potential unauthorized activities.

Comment 02-Appendix 500B table 12 - CM.01.01.01: We recommend including within the change monitoring review controls the evaluation of the completeness and accuracy of system generation of change reports/listings. Additionally, the competence and authority of the reviewers should be included because they are vital for making sure accurate evaluations of changes are implemented to the production environment.

Comment 03-Appendix 500B table 12: Considering the complexity of technology, including the new manage change methodologies such as Continuous Development/Continuous Deployment (i.e., DevOps), we recommend centralizing change management control activities within the configuration management control domain. Change controls are currently spread across Appendix 500B.

For example, interface changes, which encompass more than just configurations, are currently categorized under Business Process controls. The existing Configuration Management domain primarily addresses code changes and system security configuration changes.

Additionally, we recommend evaluating the completeness of all types of the IS components addressed in the exposure draft, including, but not limited to, changes to tools used in the automation of general control procedures and direct data changes (e.g., changes to data content/elements).

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

   Click or tap here to enter text.

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

   See our response in section 2a above.