What You Need to Know to Perform Financial Audits in 2025

Changes to the GAO/CIGIE Financial Audit Manual

PDT 2025

75 AGA

Speakers

- Robert Dacey, Chief Accountant, U.S. Government Accountability Office
- Dawn Simpson, Director, Financial Management and Assurance, U.S. Government Accountability Office
- Nicole Burkart, Assistant Director, Financial Management and Assurance, U.S. Government Accountability Office

Learning Objectives

- Identify the significant changes to the GAO/CIGIE Financial Audit Manual (FAM) and how those changes affect federal financial statement audits for 2025.
- Identify how the updated FAM financial statement audit methodology integrates information system controls assessments under GAO's Federal Information System Controls Audit Manual (FISCAM).

Overview of FAM

- FAM presents a methodology for performing financial statement audits of federal entities in accordance with professional standards.
- FAM is a three-volume publication
  - Volume 1 – Audit Methodology
  - Volume 2 – Detailed Implementation Guidance
  - Volume 3 – Federal Financial Reporting Checklist
- FAM is a joint effort between GAO and Council of the Inspectors General on Integrity and Efficiency (CIGIE).

Overview of FISCAM

- FISCAM presents a methodology for assessing information system (IS) controls.
- IS controls are those internal controls that depend on information system processing—processing performed by information systems using information technology.
  - User Controls
  - Application Controls
  - General Controls
- The 2024 revision of FISCAM became effective for engagements beginning on or after October 1, 2024.

Significant Changes to FAM Volume 1

- FAM Volume 1 changes related to the 2024 revision of FISCAM include enhanced guidance on
  - Understanding inherent risk factors related to the nature of the entity's IT environment,
  - Identifying significant business process applications and significant manual processes,
  - Considering the effect of information technology on internal control and the likelihood of effective IS controls, and
  - Identifying and assessing relevant IS controls, including general controls that address the risks arising from the use of information technology.

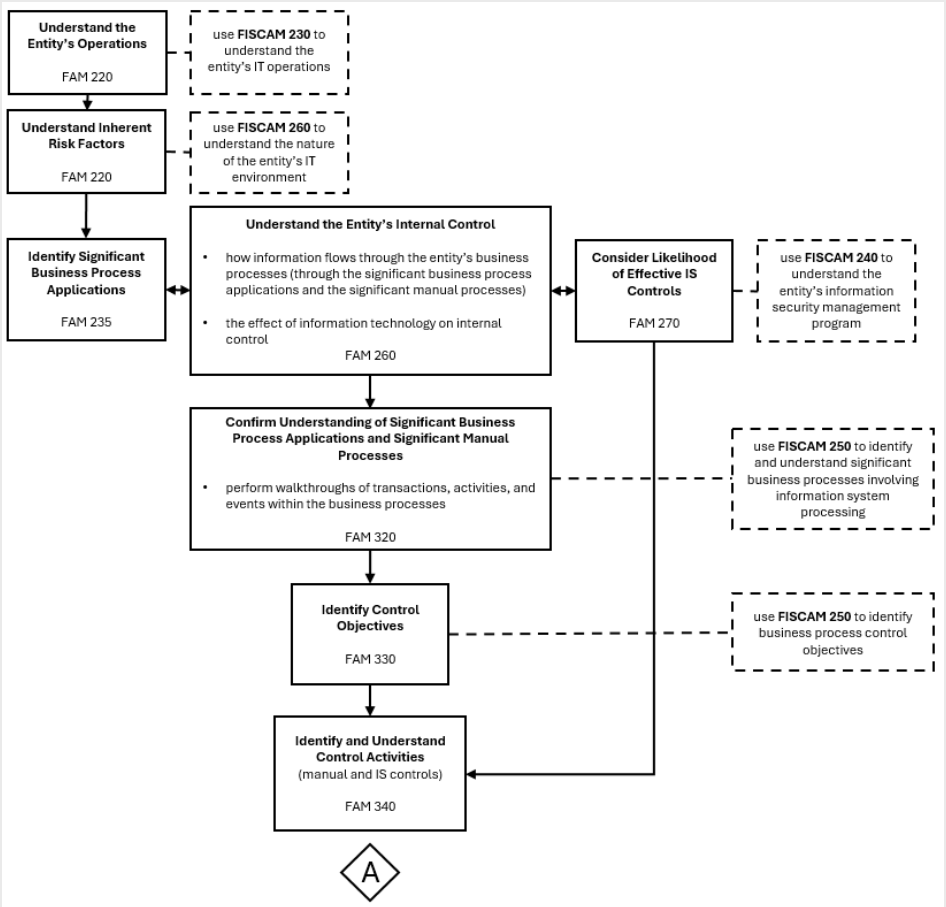
Other Changes to FAM Volume 1

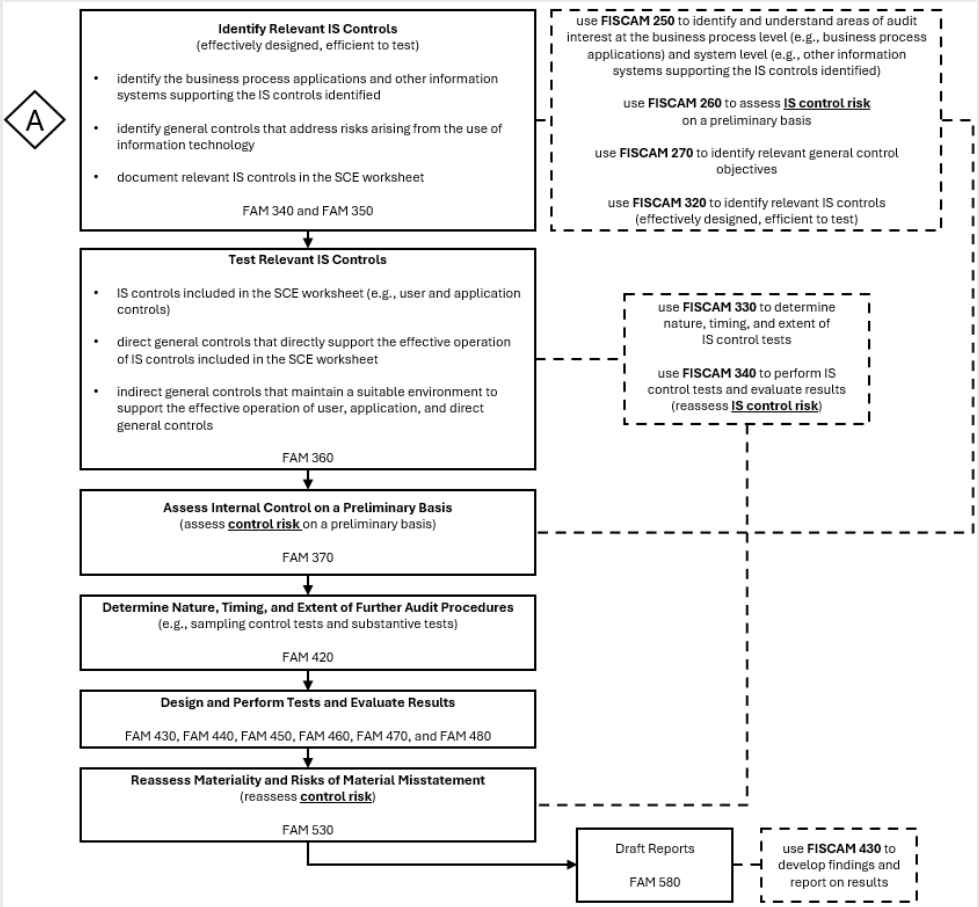
- Updates to certain terms and definitions.
- Modifications to the Specific Control Evaluation (SCE) worksheet, Line Item Risk Analysis (LIRA) form, and related instructions, including additional examples to illustrate certain concepts.
- A requirement for the auditor to obtain an understanding of how management applies the concept of materiality.
- Enhanced guidance on how the auditor should establish a clearly trivial threshold.
- Clarification that, though the auditor is not required to assess inherent risk for financial statement level risks, certain financial statement level risks may be significant risks.

Polling Question #1

- Changes to FAM Volume 1 are primarily based on the 2024 revision of FISCAM
  a. True
  b. False

Steps for Understanding and Assessing IS Controls





FAM 220 Understand the Entity's Operations

Understanding Inherent Risk Factors

- Inherent risk factors are characteristics of events or conditions that affect the susceptibility of an assertion about a line item, account, note disclosure, or class of transactions to misstatement, whether due to fraud or error, before consideration of control activities.
- Inherent risk factors incorporate characteristics of an entity, a transaction, an account, or an assertion that exist because of the
  - nature of the entity's programs,
  - prior history of audit adjustments,
  - nature of material transactions and accounts, or
  - nature of the entity's IT environment.

FAM 220 Understand the Entity's Operations

Understanding Inherent Risk Factors

- Inherent risk factors may be qualitative or quantitative and include
  - complexity,
  - subjectivity,
  - change,
  - uncertainty,
  - susceptibility to noncompliance, or
  - susceptibility to misstatement due to management bias or other fraud risk factors.

FAM 220 Understand the Entity's Operations

Understanding Inherent Risk Factors

- **Nature of the entity's IT environment**. A complex IT environment or one that is undergoing significant change may increase inherent risk. Additionally, the information technology the entity employs can introduce inherent risk factors.
- FISCAM 230 and 260 provide guidance for obtaining an understanding of the entity's IT operations and identifying IS risk factors.
  - IS risk factors are conditions or events that affect the susceptibility of the areas of audit interest (information systems included in the scope of the IS controls assessment) to information system processing errors before consideration of any mitigating IS controls.

FAM 235 Identify Significant Business Process Applications and Significant Manual Processes

- A business process is the primary means through which the entity accomplishes its mission. Business processes include both business process applications and manual processes.
  - A business process application is an IT application that helps the entity perform a specific business process or related business processes.
    - An IT application is a combination of application software, system software, and hardware designed and implemented to serve a particular function. The entity's IT applications and supporting IT infrastructure comprise the entity's information systems.
  - A manual process is a business process that does not involve the use of information technology.

FAM 235 Identify Significant Business Process Applications and Significant Manual Processes

- For material line items, accounts, note disclosures, and classes of transactions, the auditor should identify the primary business process applications and manual processes that support them (i.e., significant business process applications and significant manual processes).
  - Identifying and understanding these business process applications and manual processes helps the auditor to
    - understand the flow of transactions,
    - identify the likely sources of potential misstatements and the controls designed to address them, and
    - design control and substantive tests.

FAM 235 Identify Significant Business Process Applications and Significant Manual Processes

- FAM 260 and 320 provide guidance on obtaining an understanding of significant business process applications and significant manual processes.
- FISCAM 250 provides guidance for identifying and understanding significant business processes involving information system processing, as a basis for defining the scope of the IS controls assessment.

FAM 260 Understand the Entity's Internal Control

Considering the Effect of Information Technology on Internal Control

- The entity's use of information technology affects the manner in which the information relevant to the preparation of the financial statements is
  - processed,
  - stored, and
  - communicated and,
  - therefore, affects the manner in which the entity's internal control system is designed and implemented.

Information technology may be integrated into all five components of internal control.

FAM 260 Understand the Entity's Internal Control

Considering the Effect of Information Technology on Internal Control

- When evaluating the five components of internal control, the auditor should obtain an understanding of the entity's information security management program to consider the effect of information technology on internal control.
- FISCAM 240 provides guidance for obtaining an understanding of the entity's information security management program sufficient to
    1. assess the design and implementation of the control environment, entity risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment;
    2. assess IS control risk on a preliminary basis; and
    3. determine the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest.

FAM 260 Understand the Entity's Internal Control

Considering the Effect of Information Technology on Internal Control

- IS control risk - likelihood that conditions or events, related to the areas of audit interest, that could significantly affect the entity's ability to achieve its information processing objectives (completeness, accuracy, and validity), will not be prevented, or detected and corrected, on a timely basis by the entity's IS controls.
  - IS controls are internal controls that depend on information system processing. They include user controls, application controls, and general controls.

FAM 260 Understand the Entity's Internal Control

Considering the Effect of Information Technology on Internal Control

- The entity's information security management program is the foundation of its information security control structure and reflects senior management's commitment to addressing information security risks.
- Information security management programs provide a framework and continuous cycle of activity for
  - assigning and communicating responsibilities,
  - identifying and responding to risks,
  - developing and implementing effective information security policies,
  - monitoring the adequacy of the entity's IS controls, and
  - holding individuals and external parties accountable for their internal control responsibilities.

FAM 270 Consider Likelihood of Effective IS Controls

- Based on the auditor's understanding of the entity's information security management program, the auditor should consider whether IS controls are likely to be effective.
  - The auditor may determine that IS controls are likely to be effective in some areas and not likely to be effective in other areas.
    - For areas where the auditor believes that IS controls **are likely to be effective**, the auditor should consider specific IS controls in determining whether control objectives are achieved in the internal control phase.
    - For areas where the auditor believes that IS controls **are not likely to be effective**, the auditor should understand the impact of these ineffective IS controls on other controls.

Polling Question #2

- What are the types of IS controls?
  a. Hardware, software, and firmware
  b. User, application, and general (direct and indirect)
  c. Business process, system, and entity
  d. Manual, user, and both

PDT 2025

75 AGA

FAM 320 Confirm the Understanding of Significant Business Process Applications and Significant Manual Processes

- Walk-throughs are important for confirming the auditor's understanding of the flow of transactions, activities, and events within a business process and for designing further audit procedures.
  - In performing walk-throughs, the auditor confirms the understanding obtained in the planning phase, including
    - how information technology affects the entity's flow of transactions, and
    - the format and content of the inputs and outputs (including source documents, data files, and system-generated reports).
- FISCAM 250 provides guidance for identifying and understanding significant business processes involving information system processing and performing walk-throughs.

FAM 330 Identify Control Objectives

- To identify control objectives for financial reporting controls, the auditor considers the identified risks of material misstatement at the assertion level for which inherent risk is more than remote for each material line item, account, note disclosure, and class of transactions.
  - The auditor should prepare SCE worksheets that collectively document, for material line items, accounts, note disclosures, and classes of transactions,
    - the identified risks of material misstatement at the assertion level and
    - the control objectives and control activities that address those risks for which inherent risk is more than remote.
- The auditor should link each SCE worksheet to the related LIRA form(s).

FAM 340 Identify and Understand Control Activities

Identify IS Controls

- For each control objective identified, based on discussions with entity personnel and the results of other procedures performed, the auditor should identify the control activities that, if effectively designed, implemented, and operating, would allow management to achieve the control objective.
  - The auditor should determine whether each of the specific control activities identified is an IS control.
    - User controls
    - Application controls
    - General controls (direct and indirect)
- In FISCAM, IS controls that are directly related to a business process (i.e., user, application, and direct general controls) are referred to as business process controls.

FAM 340 Identify and Understand Control Activities

Identify the Business Process Applications and Other Information Systems Supporting the IS Controls Identified

- The auditor should identify the business process applications and other information systems supporting the IS controls identified (areas of audit interest).
  - The business process applications identified here may or may not be the same as the significant business process applications identified in FAM 235.
    - For example, for a significant business process application to be considered an area of audit interest, it will also support one or more of the IS controls identified.

FAM 340 Identify and Understand Control Activities

Identify the Risks Arising from the Use of Information Technology

- For the business process applications and other information systems identified, the auditor should identify the
  - related risks arising from the use of information technology, and
  - entity's general controls that address such risks.
- Risks arising from the use of information technology
  - affect the susceptibility of IS controls to ineffective design or operation due to ineffective general controls, and
  - are risks to the integrity of information due to ineffective IS controls.

FAM 340 Identify and Understand Control Activities

Define the Scope of the IS Controls Assessment

- FISCAM 250 provides guidance on defining the scope of the IS controls assessment
- The auditor uses the FISCAM Framework and the auditor's understanding of the business process application to identify the
  1. relevant general control objectives that, if achieved, would support the effective operation of user and application controls and
  2. direct and indirect general controls that the entity designed to achieve those objectives.

FAM 350 Determine the Nature, Timing, and Extent of Control Tests

Identify Relevant Control Activities

- For each control objective, the auditor should
  - identify control activities to test (i.e., relevant control activities);
  - perform walk-throughs to determine whether relevant control activities have been implemented;
  - document relevant control activities in the SCE worksheet or equivalent; and
  - determine the nature, timing, and extent of tests of relevant control activities.
- The auditor should determine which control activity, or combination of control activities, to test (i.e., relevant control activities) based on their ability to (1) achieve the control objective and (2) improve the efficiency of control tests.
- FISCAM 320 provides guidance for identifying relevant IS controls.

Polling Question #3

- Walk-throughs
  a. Trace one or more transactions, activities, or events through all processing
  b. Include a combination of audit procedures (i.e., observation, inspection, and inquiry)
  c. Are presentations of processes and controls provided by management to the auditor
  d. Both a. and b.

FAM 350 Determine the Nature, Timing, and Extent of Control Tests

Document Relevant Control Activities

- The auditor should document relevant control activities and whether they have been implemented in the SCE worksheet
  - For each relevant control activity listed in the SCE worksheet, the auditor should indicate whether it is an
    - IS control (i.e., depends on information system processing),
    - manual control, or
    - both.
  - IS controls listed in the SCE worksheet are generally user and application controls.
- User controls are controls that are performed by people interacting with information systems. A user control is both a manual control and an IS control if its effectiveness depends on information system processing.

FAM 350 Determine the Nature, Timing, and Extent of Control Tests

IS Controls

- FISCAM 330 provides guidance for determining the nature, timing, and extent of IS control tests.
- The nature, timing, and extent of IS control tests will vary by IS control, depending on the type of evidence available to the auditor to demonstrate whether the control is implemented and operating effectively.

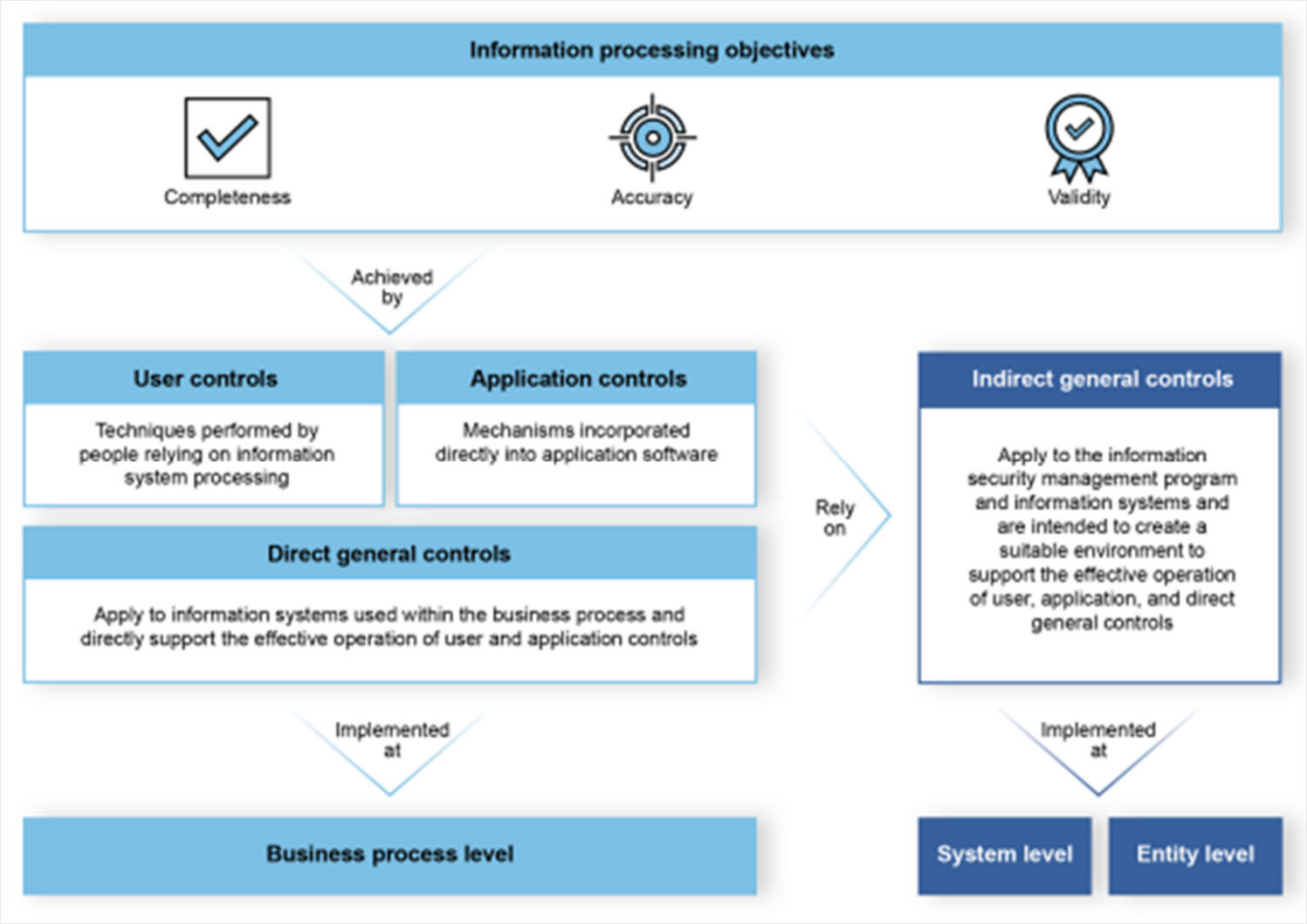
FAM 360 Perform Control Tests

Assess Relevant IS Controls

- The auditor should test the operating effectiveness of relevant control activities that have been implemented. The auditor, generally with assistance from an IS controls auditor, should assess the effectiveness of
  - IS controls included on the SCE worksheet (e.g., user and application controls); and
  - other IS controls on which the effectiveness of each IS control in the SCE worksheet depends, such as
    - direct general controls - directly support the effective operation of IS controls included on the SCE worksheet, and
    - indirect general controls - maintain a suitable environment to support the effective operation of user, application, and direct general controls.
- FISCAM 340 provides guidance for testing IS controls and evaluating the results.

FAM 360 Perform Control Tests

Assess Relevant IS Controls



FAM 360 Perform Control Tests

Assess Relevant IS Controls

- Identifying the general controls (direct and indirect) on which the effectiveness of IS controls included in the SCE worksheet depends requires
  - an understanding of the business process applications (i.e., the areas of audit interest at the business process level) and
  - the identification of areas of audit interest at the system level.

Note: Relevant (i.e., effectively designed, efficient to test) general controls are typically not listed in the SCE worksheet because they indirectly address risks of material misstatement at the assertion level by supporting the effective operation of user and application controls.

FAM 360 Perform Control Tests

Assess Relevant IS Controls

- If (1) general controls are not effectively designed or (2) relevant general controls are not implemented or are implemented but not operating effectively, the auditor may be unable to conclude that relevant user and application controls are effective.
- In such instances, the auditor should
  - determine and document the nature and extent of risks resulting from the lack of effectively designed general controls or ineffective relevant general controls,
  - identify and test any manual controls that achieve the control objectives that the IS controls in the SCE worksheet or equivalent were unable to achieve, and
  - follow the guidance in FAM 580 for classifying and reporting control deficiencies.

Polling Question #4

- Generally, the IS controls identified on the SCE worksheets are general controls, as these are more likely to address the identified risks of material misstatement at the assertion level
  a. True
  b. False

Updates to Certain Terms and Definitions

Old Terminology	New Terminology
Financial management system (when used outside of the context of FFMIA)	Business process application or manual process
Aspects of the entity's IT environment that are subject to risks arising from the use of IT	Business process applications and other information systems supporting the IS controls identified in FAM 340

- Added or revised definitions for
  - application controls, manual controls, and user controls;
  - business process, business process application, and manual process;
  - general controls (direct and indirect),
  - information security management program; and
  - information systems and areas of audit interest.

Modifications to the LIRA Form, SCE Worksheet, and Related Instructions

- Added a new column to the SCE worksheet and LIRA form to emphasize the expectation that identified risks of material misstatement are tailored to the class of transactions and specific circumstances of the entity.
- Updated the related instructions and other guidance to include additional examples illustrating concepts used in FAM
  - Expanded description and examples of line item/account-related classes of transactions.
  - Expanded description and examples of identified risks of material misstatement for classes of transactions included on the LIRA form and SCE worksheet.

Modifications to the LIRA Form, SCE Worksheet, and Related Instructions

Internal Control Phase
395 H – Line Item Risk Analysis Form

Note: For illustrative purposes, some columns contain example text. The auditor should complete all columns as applicable.

ENTITY: _____
DATE OF FINANCIAL STATEMENTS: _____
LINE ITEM & TOTAL:[22] [e.g., Cash $100,000,000]
ACCOUNTS & BALANCES: _____
NOTE DISCLOSURES: _____

LINE ITEM RISK ANALYSIS

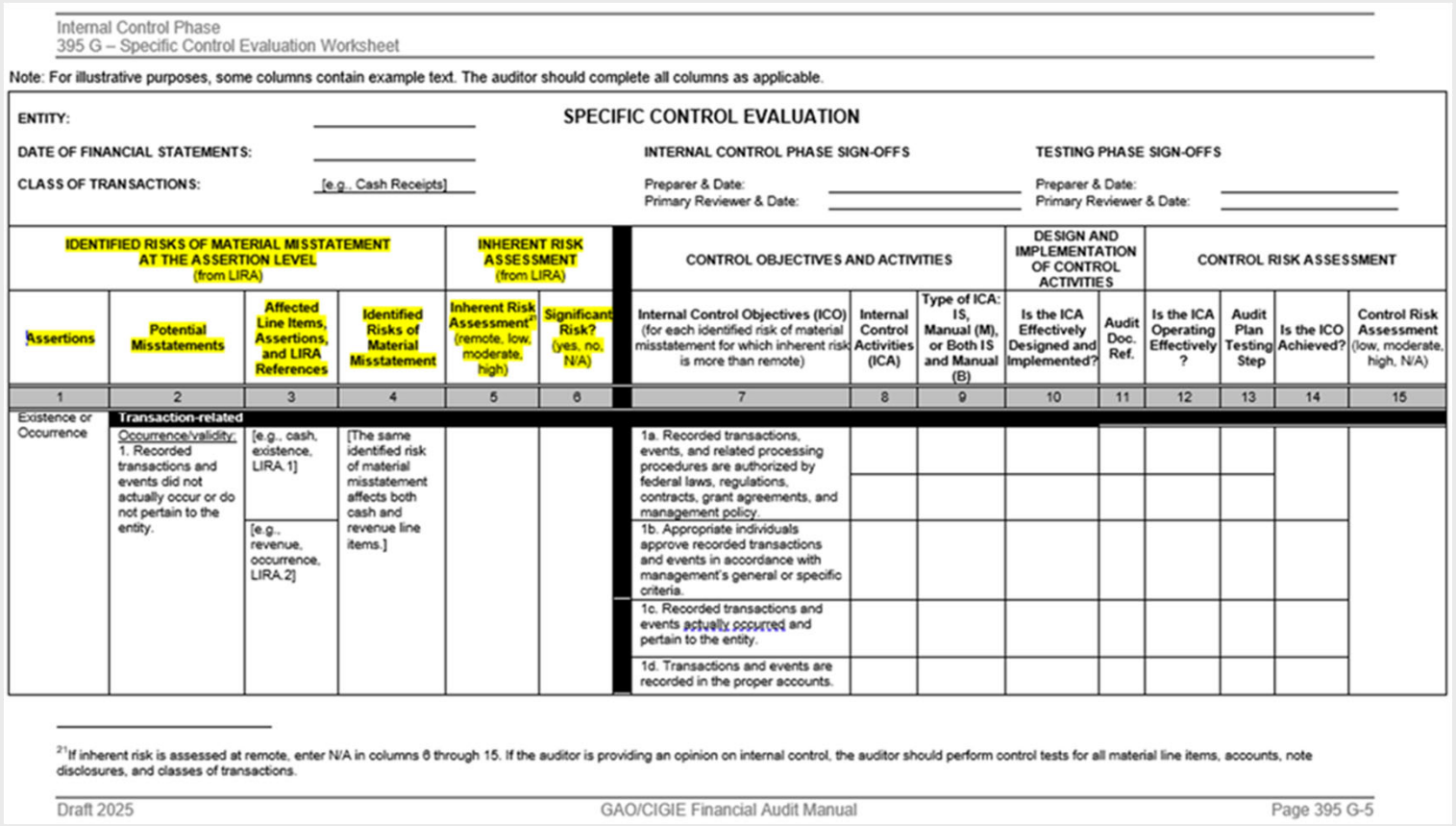
Preparer and Date: _____
Primary Reviewer and Date: _____

PLANNING PHASE							INTERNAL CONTROL PHASE		TESTING PHASE	
IDENTIFIED RISKS OF MATERIAL MISSTATEMENT AT THE ASSERTION LEVEL				INHERENT RISK ASSESSMENT			CONTROL RISK ASSESSMENT from SCEs (low, moderate, high, N/A)	RISK OF MATERIAL MISSTATEMENT ASSESSMENT Combined Inherent Risk and Control Risk (low, moderate, high, N/A)	SUBSTANTIVE AUDIT PROCEDURES	
Assertions	**Potential Misstatements**	**Classes of Transactions & SCE References**	**Identified Risks of Material Misstatement**	**Inherent Risk Considerations** (including fraud risk and noncompliance considerations)	**Inherent Risk Assessment** (remote, low, moderate, high)[23]	**Significant Risk?** (yes, no, N/A)			**Nature, Timing, & Extent**	**Audit Plan Testing Step**
1	2	3	4	5	6	7	8	9	10	11
Existence or Occurrence	**Transaction-related**									
	Occurrence/validity 1. Recorded transactions and events did not actually	[e.g., cash receipts, SCE.1]	[columns 4 - 11 would be consistent with the applicable revenue/accounts receivable LIRA related to cash receipts]						[e.g., see revenue LIRA]	

[22] The auditor should include a note on the LIRA form to explain what these amounts represent (e.g., prior-year reported amounts, current-year projected amounts based on interim information, or other amounts). If the actual reported amounts for the current year materially differ from the amounts initially listed, the auditor should update those amounts accordingly.

[23] If inherent risk is assessed at remote, enter N/A for columns 7 through 11. If inherent risk is remote for all identified risks of material misstatement, see FAM 395 H.03 for instructions.

Modifications to the LIRA Form, SCE Worksheet, and Related Instructions



Internal Control Phase
395 G – Specific Control Evaluation Worksheet

Note: For illustrative purposes, some columns contain example text. The auditor should complete all columns as applicable.

ENTITY: _____ **SPECIFIC CONTROL EVALUATION**

DATE OF FINANCIAL STATEMENTS: _____ **INTERNAL CONTROL PHASE SIGN-OFFS** **TESTING PHASE SIGN-OFFS**

CLASS OF TRANSACTIONS: [e.g., Cash Receipts] Preparer & Date: _____ Preparer & Date: _____
Primary Reviewer & Date: _____ Primary Reviewer & Date: _____

IDENTIFIED RISKS OF MATERIAL MISSTATEMENT AT THE ASSERTION LEVEL (from LIRA)				INHERENT RISK ASSESSMENT (from LIRA)		CONTROL OBJECTIVES AND ACTIVITIES			DESIGN AND IMPLEMENTATION OF CONTROL ACTIVITIES		CONTROL RISK ASSESSMENT			
Assertions	Potential Misstatements	Affected Line Items, Assertions, and LIRA References	Identified Risks of Material Misstatement	Inherent Risk Assessment[2] (remote, low, moderate, high)	Significant Risk? (yes, no, N/A)	Internal Control Objectives (ICO) (for each identified risk of material misstatement for which inherent risk is more than remote)	Internal Control Activities (ICA)	Type of ICA: IS, Manual (M), or Both IS and Manual (B)	Is the ICA Effectively Designed and Implemented?	Audit Doc. Ref.	Is the ICA Operating Effectively?	Audit Plan Testing Step	Is the ICO Achieved?	Control Risk Assessment (low, moderate, high, N/A)
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Existence or Occurrence	**Transaction-related**													
	Occurrence/validity: 1. Recorded transactions and events did not actually occur or do not pertain to the entity.	[e.g., cash, existence, LIRA.1]	[The same identified risk of material misstatement affects both cash and revenue line items.]			1a. Recorded transactions, events, and related processing procedures are authorized by federal laws, regulations, contracts, grant agreements, and management policy.								
		[e.g., revenue, occurrence, LIRA.2]				1b. Appropriate individuals approve recorded transactions and events in accordance with management's general or specific criteria.								
						1c. Recorded transactions and events actually occurred and pertain to the entity.								
						1d. Transactions and events are recorded in the proper accounts.								

[2] If inherent risk is assessed at remote, enter N/A in columns 6 through 15. If the auditor is providing an opinion on internal control, the auditor should perform control tests for all material line items, accounts, note disclosures, and classes of transactions.

Draft 2025 GAO/CIGIE Financial Audit Manual Page 395 G-5

PDT 2025

75 AGA

New Requirement to Understand How Management Applies Materiality

- The materiality levels that the auditor sets in the planning phase are intended to be used by the auditor, not management.
- Management and the auditor have different objectives when considering materiality.
  - Management's objective is to consider materiality in the fair presentation of the financial statements.
  - The auditor's objective in planning is to determine the nature, timing, and extent of audit procedures in order to obtain sufficient appropriate audit evidence on which to base the audit opinion.
- The auditor should obtain an understanding of how management applies the concept of materiality and how it affects the auditor's identification and assessment of the risks of material misstatement as discussed in FAM 265.

Enhanced Guidance on Establishing a Clearly Trivial Threshold

- The clearly trivial amount set by the auditor should be substantially below performance materiality so that the aggregate of many items at the clearly trivial amount would not exceed performance materiality.
- To support the aggregation of many misstatements, the auditor generally should use a threshold that is 5 percent (or less) of performance materiality.
- The auditor should document the rationale for using a higher percentage, based on the facts and circumstances of the entity.

Clarification that Certain Financial Statement Level Risks May Be Significant Risks

- A significant risk is an identified risk of material misstatement
  - for which the assessment of inherent risk is high (based on AU-C 315);
  - due to fraud, for which inherent risk is more than remote (AU-C 240.27); or
  - arising from transactions with disclosure entities, related parties, and public-private partnerships that are also significant unusual transactions, for which inherent risk is more than remote (AU-C 550.20).
- AU-C 315 does not require the auditor to assess inherent risk for financial statement level risks; however, certain financial statement level risks may be significant risks based on other standards (e.g., AU-C 240 and 550). Also, financial statement level risks may affect the auditor's assessment of significant risks at the assertion level.

Thank you for your participation.

Questions? Please contact us at:

FAM@gao.gov

FISCAM@gao.gov

PDT 2025

75 AGA