SECTION 200

Planning Phase

Figure 200.1: Methodology Overview

Planning Phase	Section
• Understand the entity's operations	220
• Perform preliminary analytical procedures	225
• Determine planning, design, and test materiality	230
• Identify significant line items, accounts, assertions and RSSI	235
• Identify significant cycles, accounting applications, and financial management systems	240
• Identify significant provisions of laws and regulations	245
• Identify relevant budget restrictions	250
• Assess risk factors	260
• Determine likelihood of effective information system controls	270
• Identify relevant operations controls to evaluate and test	275
• Plan other audit procedures	280
• Plan locations to visit	285

Internal Control Phase	Section
• Understand information systems	320
• Identify control objectives	330
• Identify and understand relevant control activities	340
• Determine the nature, timing, and extent of control tests and of tests for systems' compliance with FFMIA requirements	350
• Perform nonsampling control tests and tests for systems' compliance with FFMIA requirements	360
• Assess controls on a preliminary basis	370

Testing Phase	Section
• Consider the nature, timing, and extent of tests	420
• Design efficient tests	430
• Perform tests and evaluate results	440
•• Sampling control tests	450
•• Compliance tests	460
•• Substantive tests	470
••• Substantive analytical procedures	475
••• Substantive detail tests	480

Reporting Phase	Section
• Perform overall analytical procedures	520
• Determine adequacy of audit procedures and audit scope	530
• Evaluate misstatements	540
• Conclude other audit procedures:	550
•• Inquire of attorneys	
•• Consider subsequent events	
•• Obtain management representations	
•• Consider related party transactions	
• Determine conformity with generally accepted accounting principles	560
• Determine compliance with GAO/PCIE *Financial Audit Manual*	570
• Draft reports	580

210 - OVERVIEW

.01 The auditor performs planning to determine an effective and efficient way to obtain the evidential matter necessary to report on the entity's Accountability Report (or annual financial statement). The nature, extent, and timing of planning varies with, for example, the entity's size and complexity, the auditor's experience with the entity, and the auditor's knowledge of the entity's operations. Procedures performed in the planning phase are shown in figure 200.1.

.02 A key to a quality audit, planning requires the involvement of senior members of the audit team. Although concentrated in the planning phase, planning is an iterative process performed throughout the audit. For example, findings from the internal control phase directly affect planning the substantive audit procedures. Also, the results of control and substantive tests may require changes in the planned audit approach.

.03 Auditors should consider the needs of, and consult in a timely manner with, other auditors who plan to use the work being performed, especially when making decisions that require the auditor to exercise significant judgment.

[This page intentionally left blank.]

220 - UNDERSTAND THE ENTITY'S OPERATIONS

.01 The auditor should obtain an understanding of the entity sufficient to plan and perform the audit in accordance with applicable auditing standards and requirements. In planning the audit, the auditor gathers information to obtain an overall understanding of the entity and its origin and history, size and location, organization, mission, business, strategies, inherent risks, fraud risks, control environment, risk assessment, communications, and monitoring. Understanding the entity's operations in the planning process enables the auditor to identify, respond to, and resolve accounting and auditing problems early in the audit.

.02 The auditor's understanding of the entity and its operations does not need to be comprehensive but should include:

- entity management and organization,
- external factors affecting operations,
- internal factors affecting operations, and
- accounting policies and issues.

.03 The auditor should identify key members of management and obtain a general understanding of the organizational structure. The auditor's main objective is to understand how the entity is managed and how the organization is structured for the particular management style.

.04 The auditor should identify significant external and internal factors that affect the entity's operations. External factors might include (1) source(s) of funds, (2) seasonal fluctuations, (3) current political climate, and (4) relevant legislation. Internal factors might include (1) size of the entity, (2) number of locations, (3) structure of the entity (centralized or decentralized), (4) complexity of operations, (5) information system structure, (6) qualifications and competence of key personnel, and (7) turnover of key personnel.

.05 In identifying accounting policies and issues, the auditor should consider

- generally accepted accounting principles, including whether the entity is likely to be in compliance;
- changes in GAAP that affect the entity; and

- whether entity management appears to follow aggressive or conservative accounting policies.

.06 The auditor also should consider whether the entity will report any required supplementary stewardship information (RSSI). This includes stewardship property, plant, and equipment (PP&E) (heritage assets, national defense assets, and stewardship land), stewardship investments (nonfederal physical property, human capital, and research and development), social insurance, and risk-assumed information. RSSI and deferred maintenance, which is considered required supplementary information, should be designated "unaudited."

.07 The auditor should develop and document a high-level understanding of the entity's use of information systems (IS) and how IS affect the generation of financial statement information, RSSI, and the data that support performance measures reported in the MD&A (overview) of the Accountability Report (CFO report). An IS auditor may assist the auditor in understanding the entity's use of IS. Appendix I of the GAO *Federal Information System Controls Manual* (FISCAM) can be used to document this understanding.

.08 The auditor gathers planning information through different methods (observation, interviews, reading policy and procedure manuals, etc.) and from a variety of sources, including

- top-level entity management,
- entity management responsible for significant programs,
- Office of Inspector General (IG) and internal audit management (including any internal control officer),
- others in the audit organization concerning other completed, planned or in-progress assignments,
- personnel in OGC,
- personnel in the Special Investigator Unit, and
- entity legal representatives.

.09 The auditor gathers information from relevant reports and articles issued by or about the entity, including

- the entity's prior Accountability Reports;
- other financial information;
- FMFIA reports and supporting documentation;
- reports by management or the auditor about systems' substantial compliance with FFMIA requirements;
- the entity's budget and related reports on budget execution;
- GAO reports;
- IG and internal audit reports (including those for performance audits and other reviews);
- congressional hearings and reports;
- consultant reports; and
- material published about the entity in newspapers, magazines, internet sites, and other publications.

[This page intentionally left blank.]

225 - PERFORM PRELIMINARY ANALYTICAL PROCEDURES

.01 During the planning phase, preliminary analytical procedures are performed to help the auditor

- understand the entity's business, including current-year transactions and events;
- identify account balances, transactions, ratios, or trends that may signal inherent or control risks, including any risks related to fraud (see section 260);
- identify and understand the significant accounting policies;
- determine planning, design, and test materiality (see section 230); and
- determine the nature, timing, and extent of audit procedures to be performed.

.02 GAAS requires the auditor to perform preliminary analytical procedures (AU 329). The resources spent in performing these procedures should be commensurate with the expected reliability of comparative information. For example, in a first-year audit, comparative information might be unreliable; therefore, preliminary analytical procedures generally should be limited.

.03 The auditor generally should perform the following steps to achieve the objectives of preliminary analytical procedures:

a. **Compare current-year amounts with relevant comparative financial information:** The financial data used in preliminary analytical procedures generally are summarized at a high level, such as the level of financial statements. If financial statements are not available, the budget or financial summaries that show the entity's financial position and results of operations may be used.

   The auditor compares current-year amounts with relevant comparative financial information. Use of unaudited comparative data might not allow the auditor to identify significant fluctuations, particularly if an item consistently has been treated incorrectly. Also, the auditor may identify fluctuations that are not really fluctuations due to errors in the unaudited comparative data.

   A key to effective preliminary analytical procedures is to use information that is comparable in terms of the time period presented and the presentation (i.e., same level of detail and consistent grouping of detail accounts into summarized amounts used for comparison).

   The auditor may perform ratio analysis on current-year data and compare the current year's ratios with those derived from prior periods or budgets. The

auditor does this to study the relationships among components of the financial statements and to increase knowledge of the entity's activities. The auditor uses ratios that are relevant indicators or measures for the entity. Also, the auditor should consider any trends in the performance indicators prepared by the entity.

b. **Identify significant fluctuations:** Fluctuations are differences between the recorded amounts and the amounts expected by the auditor, based on comparative financial information and the auditor's knowledge of the entity. Fluctuations refer to both unexpected differences between current-year amounts and comparative financial information as well as the absence of expected differences. The identification of fluctuations is a matter of the auditor's judgment.

   The auditor establishes parameters for identifying significant fluctuations. When setting these parameters, the auditor generally considers the amount of the fluctuation in terms of absolute size and/or the percentage difference. The amount and percentage used are left to the auditor's judgment. An example of a parameter is "All fluctuations in excess of $10 million and/or 15 percent of the prior-year balance or other unusual fluctuations will be considered significant."

c. **Inquire about significant fluctuations:** The auditor discusses the identified fluctuations with appropriate entity personnel. The focus of the discussion is to achieve the purposes of the procedures described in paragraph 225.01. For preliminary analytical procedures, the auditor does not need to corroborate the explanations since they will be tested later. However, the explanations should appear reasonable and consistent to the auditor. The inability of entity personnel to explain the cause of a fluctuation may indicate the existence of control, fraud, and/or inherent risks.

.04 In performing preliminary analytical procedures, the auditor develops expectations about plausible relationships that are expected to exist. Because these procedures generally use data aggregated at a high level, their results typically provide only a broad initial indication about a potential misstatement. The auditor should consider any unusual relationships, together with other information gathered, in identifying the risk of material misstatement due to fraud (see section 260).

230 - DETERMINE PLANNING, DESIGN, AND TEST MATERIALITY

.01 Materiality is one of several tools the auditor uses to determine that the planned nature, timing, and extent of procedures are appropriate. As defined in Financial Accounting Standards Board (FASB) Statement of Financial Concepts No. 2., materiality represents the magnitude of an omission or misstatement of an item in a financial report that, in light of surrounding circumstances, makes it probable that the judgment of a reasonable person relying on the information would have been changed or influenced by the inclusion or correction of the item.

.02 Materiality is based on the concept that items of little importance, which do not affect the judgment or conduct of a reasonable user, do not require auditor investigation. Materiality has both quantitative and qualitative aspects. Even though quantitatively immaterial, certain types of misstatements could have a material impact on or warrant disclosure in the financial statements for qualitative reasons.

.03 For example, intentional misstatements or omissions (fraud) usually are more critical to the financial statement users than are unintentional errors of equal amounts. This is because the users generally consider an intentional misstatement more serious than clerical errors of the same amount.

.04 GAGAS and incorporated GAAS require the auditor to consider materiality in planning, designing procedures, and considering need for disclosure in the audit report. AU 312 requires the auditor, in planning the audit, to consider his/her preliminary judgment about materiality levels. The "yellow book" states that materiality is a matter of professional judgment influenced by the needs of the reasonable person relying on the financial statements. Materiality judgments are made in the light of surrounding circumstances and involve both quantitative and qualitative considerations, such as the public accountability of the auditee and the visibility and sensitivity of government programs, activities, and functions.

.05 The term "materiality" can have several meanings. In planning and performing the audit, the auditor uses the following terms that relate to materiality:

- **Planning materiality** is a preliminary estimate of materiality, in relation to the financial statements taken as a whole, used to determine the nature, timing, and extent of substantive audit procedures and to identify significant laws and regulations for compliance testing.

- **Design Materiality** is the portion of planning materiality that has been allocated to line items, accounts, or classes of transactions (such as disbursements). This amount will be the same for all line items or accounts (except for certain intragovernmental or offsetting balances as discussed in paragraph 230.10).

- **Test materiality** is the materiality actually used by the auditor in testing a specific line item, account, or class of transactions. Based on the auditor's judgment, test materiality can be equal to or less than design materiality, as discussed in paragraph 230.13. Test materiality may be different for different line items or accounts.

.06 The following other uses of the term "materiality" relate principally to the reporting phase:

- **Disclosure materiality** is the threshold for determining whether an item should be reported or presented separately in the financial statements or in the related notes. This value may differ from planning materiality.

- **FMFIA materiality** is the threshold for determining whether a matter meets OMB criteria for reporting matters under FMFIA as described in paragraphs 580.35-.37.

- **Reporting materiality** is the threshold for determining whether an unqualified opinion can be issued. In the reporting phase, the auditor considers whether unadjusted misstatements are quantitatively or qualitatively material. If considered to be material, the auditor would be precluded from issuing an unqualified opinion on the financial statements. See section 540.

Unless otherwise specified, such as through using the terms above, the term "materiality" in this manual refers to the overall financial statement materiality as defined in paragraph 230.01.

.07 The following guidelines provide the auditor with a framework for determining planning materiality. <u>However, this framework is not a substitute for professional judgment</u>. The auditor has the flexibility to determine planning materiality outside of these guidelines. In such circumstances, the Audit Director should discuss the basis for the determination with the Reviewer. The planning materiality selected and method of determining planning materiality should be documented and approved by the Audit Director.

.08 The auditor should estimate planning materiality in relation to the element of the financial statements that is most significant to the primary users of the statements (the materiality base). The auditor uses judgment in determining the appropriate element of the financial statements to use as the materiality base. Also, since the materiality base normally is based on unaudited preliminary information determined in the planning phase, the auditor usually has to estimate the year-end balance of the materiality base. To provide reasonable assurance that sufficient audit procedures are performed, any estimate of the materiality base should use the low end of the range of estimated materiality so that sufficient testing is performed.

.09 For capital-intensive entities, total assets may be an appropriate materiality base. For expenditure-intensive entities, total expenses may be an appropriate materiality base. Based on these concepts, <u>the materiality base generally should be the greater of total assets or expenses (net of adjustments for intragovernmental balances and offsetting balances)</u>. (See discussion of these adjustments in next paragraph.) Other materiality bases that might be considered include total liabilities, equity, revenues, and net cost to the government (appropriations).

.10 In considering a materiality base, the auditor should consider how to handle significant intragovernmental balances (such as funds with the U.S. Treasury, U.S. Treasury securities, and interentity balances) and offsetting balances (such as future funding sources that offset certain liabilities and collections that are offset by transfers to other government entities). The auditor should establish a separate materiality base for significant intragovernmental or offsetting balances because combining all accounts may improperly distort the nature, timing, and extent of audit procedures. For example, an entity that collects and remits funds on behalf of other federal entities could have operating accounts that are small in comparison to the funds processed on behalf of other entities. In this example, the

auditor would compute separate planning materiality for auditing (1) the offsetting accounts, using the balance of the offsetting accounts as the materiality base and (2) the rest of the financial statements using the materiality base guidance in paragraph 230.09.

.11 Planning materiality generally should be 3 percent of the materiality base. Although a mechanical means might be used to compute planning materiality, the auditor should use judgment in evaluating whether the computed level is appropriate. The auditor also should consider adjusting the materiality base for the impact of such items as unrecorded liabilities, contingencies, and other items that are not incorporated in the entity's financial statements (and not reflected in the materiality base) but that may be important to the financial statement user.

.12 Design materiality for the audit should be one-third of planning materiality to allow for the precision of audit procedures. This guideline recognizes that misstatements may occur throughout the entity's various accounts. The design materiality represents the materiality used as a starting point to design audit procedures for line items or accounts so that an aggregate material misstatement in the financial statements will be detected, for a given level of audit assurance (discussed in paragraph 260.04).

.13 Generally, the test materiality used for a specific test is the same as the design materiality. However, the auditor may use a test materiality lower than the design materiality for substantive testing of specific line items and assertions (which increases the extent of testing) when

- the audit is being performed at some, but not all, entity locations (requiring increased audit assurance for those locations visited - see section 285);

- the area tested is deemed to be sensitive to the financial statement users; or

- the auditor expects to find a significant amount of misstatements.[1]

[1] If the auditor uses software to calculate sample size, he or she should understand how the software considers expected misstatements. For example, if the auditor uses Interactive Data Extraction and Analysis (IDEA) to calculate sample size when test materiality is lower than design materiality, because the auditor expects misstatements, the auditor should use design materiality in IDEA because he or she separately inputs the expected misstatement. See paragraph 480.27.

[This page intentionally left blank.]

235 - IDENTIFY SIGNIFICANT LINE ITEMS, ACCOUNTS, ASSERTIONS, AND RSSI

.01 The auditor should identify significant line items and accounts in the financial statements and significant related financial statement assertions. The auditor should also identify significant RSSI.[1] In the internal control and testing phases, the auditor performs control and substantive tests for each significant assertion for each significant account. By identifying significant line items, accounts, and the related assertions early in the planning process, the auditor is more likely to design efficient audit procedures. Some insignificant line items, accounts, and assertions may not warrant substantive audit tests to the extent that they are not significant in the aggregate. However, some line items and accounts with zero or unusual balances may warrant testing, especially with regard to the completeness assertion.

.02 Financial statement assertions, as defined by AU 326, are management representations that are embodied in financial statement components. Most of the auditor's work in forming an opinion on financial statements consists of obtaining and evaluating evidential matter concerning the assertions in such financial statements. The assertions can be either explicit or implicit and can be classified into the following broad categories:

- **Existence or occurrence:** An entity's assets or liabilities exist at a given date, and recorded transactions have occurred during a given period.
- **Completeness:** All transactions and accounts that should be presented in the financial statements are so included.
- **Rights and obligations:** Assets are the rights of the entity, and liabilities are the obligations of the entity at a given date.
- **Valuation or allocation:** Asset, liability, revenue, and expense components have been included in the financial statements at appropriate amounts.

---

[1] The auditor is not required to opine on RSSI, but, per OMB audit guidance, internal control over RSSI should be tested the same as internal control over the financial statements.

- **Presentation and disclosure:** The particular components of the financial statements are properly classified, described, and disclosed.

.03 A line item or an account in the financial statements or RSSI should be considered significant if it has one or more of the following characteristics:

- Its balance is material (exceeds design materiality) or comprises a significant portion of a material financial statement or RSSI amount.
- A high combined risk (inherent and control risk, as discussed in paragraph 260.02) of material misstatement (either overstatement or understatement) is associated with one or more assertions relating to the line item or account. For example, a zero or unusually small balance account may have a high risk of material understatement.
- Special audit concerns, such as regulatory requirements, warrant added consideration.

The auditor should determine that any accounts considered insignificant are not significant in the aggregate.

.04 An assertion is significant if misstatements in the assertion could exceed test materiality for the related line item, account, or disclosure. Certain assertions for a specific line item or account, such as completeness and disclosure, could be significant even though the recorded balance of the related line item or account is not material. For example, (1) the completeness assertion could be significant for an accrued payroll account with a high combined risk of material understatement even if its recorded balance is zero and (2) the disclosure assertion could be significant for a contingent liability even if no amount is recordable.

.05 Assertions are likely to vary in degree of significance, and some assertions may be insignificant or irrelevant for a given line item or account. For example:

- The completeness assertion for liabilities may be of greater significance than the existence assertion for liabilities.

- All assertions related to an account that is not significant (as defined in paragraph 235.03) are considered to be insignificant.

- The rights and obligations assertion for a revenue or expense account is irrelevant.

.06 Significant line items, accounts, and assertions should be identified in the Account Risk Analysis (ARA) or other appropriate audit planning workpapers.

[This page intentionally left blank.]

240 - IDENTIFY SIGNIFICANT CYCLES, ACCOUNTING APPLICATIONS, AND FINANCIAL MANAGEMENT SYSTEMS

.01 In the internal control phase, the auditor evaluates controls for each significant cycle and accounting application and determines whether significant financial management systems substantially comply with federal financial management systems requirements, federal accounting standards, and the SGL at the transaction level. A cycle or an accounting application should be considered significant if it processes an amount of transactions in excess of design materiality or if it supports a significant account balance in the financial statements or significant RSSI. A financial management system generally consists of one or more accounting applications. If one or more of the accounting applications making up a financial management system are considered significant, then that financial management system generally should be considered significant for determining whether the system substantially complies with FFMIA requirements. The auditor may identify other cycles, accounting applications, or financial management systems as significant based on qualitative considerations. For example, financial management systems covered by FFMIA include not only systems involved in processing financial transactions and preparing financial statements, but also systems supporting financial planning, management reporting, or budgeting activities, systems accumulating and reporting cost information, and the financial portion of mixed systems, such as benefit payment, logistics, personnel, and acquisition systems.

.02 The entity's accounting system may be viewed as consisting of logical groupings of related transactions and activities, or accounting applications. Each significant line item/account is affected by input from one or more accounting applications (sources of debits or credits). Related accounting applications may be grouped into cycles by the auditor and into financial management systems by the entity. Accounting applications are classified as (1) transaction-related or (2) line item/account-related.

.03 A transaction-related accounting application consists of the methods and records established to identify, assemble, analyze, classify, and record (in the general ledger) a particular type of transaction. Typical transaction-related accounting applications include billing, cash receipts, purchasing, cash disbursements, and payroll. A line item/account-related accounting application consists of the methods and records established to report an

entity's recorded transactions and to maintain accountability for related assets and liabilities. Typical line item/account-related accounting applications include cash balances, accounts receivable, inventory control, property and equipment, and accounts payable.

.04 Within a given entity, there may be several examples of each accounting application. For example, a different billing application may exist for each program that uses a billing process. Accounting applications that process a related group of transactions and accounts comprise cycles. For instance, the billing, returns, cash receipts, and accounts receivable accounting applications might be grouped to form the revenue cycle. Similarly, related accounting applications also comprise financial management systems.

.05 For each significant line item and account, the auditor should use the Account Risk Analysis form (ARA) (see section 395 I) or an equivalent workpaper to document the significant transaction cycles (such as revenue, purchasing, and production) and the specific significant accounting applications that affect these significant line items and accounts. For example, the auditor might determine that billing, returns, cash receipts, and accounts receivable are significant accounting applications that affect accounts receivable (a significant line item). The Account Risk Analysis form provides a convenient way for documenting the specific risks of misstatement for significant line items for consideration in determining the nature, timing, and extent of audit procedures. If an equivalent workpaper is used, rather than the ARA, it should document the information discussed in section 395 I.

.06 Related accounting applications may be grouped into cycles to aid in preparing workpapers. This helps the auditor design audit procedures that are both efficient and relevant to the reporting objectives. The auditor may document insignificant accounts in each line item on the ARA or equivalent, indicating their insignificance and consequent lack of audit procedures applied to them. In such instances, the cycle matrix may not be necessary. Otherwise, the auditor should prepare a cycle matrix or equivalent document that links each of the entity's accounts (in the chart of accounts) to a cycle, an accounting application, and a financial statement or RSSI line item.

.07 Based on discussions with entity personnel, the auditor should determine the accounting application that is the best source of the financial statement information. When a significant line item has more than one source of

financial data, the auditor should consider the various sources and determine which is best for financial audit purposes. The auditor needs to consider the likelihood of misstatement and auditability in choosing the source to use. For audit purposes, the best source of financial information sometimes may be operational information prepared outside the accounting system.

.08 Once the significant accounting applications are identified, the auditor determines which computer systems are involved in those applications. Those particular computer systems are then considered in assessing computer-related controls using an appropriate methodology.

.09 An appropriate methodology would require the auditor to obtain sufficient knowledge of the information system relevant to financial reporting to understand the accounting processing from initiation of a transaction to its inclusion in the financial statements, including electronic means used to transmit, process, maintain, and access information (see AU 319.49, SAS 94). AU 319.61 requires documentation of this understanding. OMB audit guidance notes that the components of internal control include general and application controls. General controls are the entitywide security management program, access control, application software development and change control, system software control, segregation of duties, and service continuity control. Application controls are authorization control, completeness control, accuracy control, and control over integrity of processing and data files. OMB audit guidance also requires that, for controls that have been properly designed and placed in operation, the auditor shall perform sufficient tests to support a low assessed level of control risk. The auditor should document the basis for believing that the methodology used is appropriate to satisfy these requirements for assessing general and application controls. The GAO *Federal Information System Controls Audit Manual* (FISCAM) is designed to meet these requirements. See section 295 J for a flowchart of steps generally followed in assessing information system controls in a financial statement audit. IS security controls are also addressed in OMB Circular A-130, *Management of Federal Information Resources,* in the National Institute of Standards and Technology's *An Introduction to Computer Security: The NIST Handbook*, and in other publications.

[This page intentionally left blank.]

245 - IDENTIFY SIGNIFICANT PROVISIONS OF LAWS AND REGULATIONS

.01 To design relevant compliance-related audit procedures, the auditor identifies the significant provisions of laws and regulations. To aid the auditor in this process, this manual classifies provisions of laws and regulations into the following categories:

- **Transaction-based provisions** are those for which compliance is determined on individual transactions. For example, the Prompt Payment Act requires that late payments be individually identified and interest paid on such late payments.

- **Quantitative-based provisions** are those that require the accumulation/summarization of quantitative information for measurement. These provisions may contain minimum, maximum, or targeted amounts (restrictions) for the accumulated/summarized information. For example, the Comprehensive Environmental Response, Compensation, and Liability Act of 1980 prohibits the Environmental Protection Agency from exceeding certain spending limits on specific projects.

- **Procedural-based provisions** are those that require the entity to implement policies or procedures to achieve certain objectives. For example, the Single Audit Act, as amended, requires the awarding entity to review certain financial information on awardees.

.02 The auditor should identify the significant provisions of laws and regulations. For each significant provision, the auditor should study and evaluate related compliance controls and should test compliance with the provision. To identify such significant provisions, the auditor should take these steps:

a. The auditor should review the lists of laws and regulations that OMB and the entity have determined might be significant to others. The OMB list is provided in an appendix of OMB's audit guidance and is included in section 295 H. The entity is expected to develop a list that, for CFO Act agencies and components listed in OMB audit guidance, should include laws and regulations in OMB audit guidance, whether or not they are material to the entity, because they have been determined to be

material to the consolidated financial statements of the United States Government. In addition, the auditor should identify (with OGC assistance) any laws or regulations (in addition to those identified by OMB and the entity) that have a direct effect on determining amounts in the financial statements. The meaning of direct effect is discussed below in paragraph 245.03.

b. For each such law or regulation, the auditor should identify those provisions that are significant. A provision should be considered significant if (1) compliance with the provision can be measured objectively and (2) it meets one of the following criteria for determining that the provision has a material effect on determining financial statement amounts:

- **Transaction-based provisions:** Transactions processed by the entity that are subject to the provision exceed planning materiality in the aggregate.
- **Quantitative-based provisions:** The quantitative information required by the provision or by established restrictions exceeds planning materiality.
- **Procedural-based provisions:** The provision broadly affects all or a segment of the entity's operations that process transactions exceeding planning materiality in the aggregate. For example, a provision may require that the entity establish procedures to monitor the receipt of certain information from grantees; in determining whether to test compliance with this provision, the auditor should consider whether the total amount of money granted exceeded planning materiality.

.03 A direct effect means that the provision specifies

- the nature and/or dollar amount of transactions that may be incurred (such as obligation, outlay, or borrowing restrictions),
- the method used to record such transactions (such as revenue recognition policies), or

- the nature and extent of information to be reported or disclosed in the annual financial statements (such as the statement of budgetary resources).

For example, entity-enabling legislation may contain provisions that limit the nature and amount of obligations or outlays and therefore have a direct effect on determining amounts in the financial statements. If a provision's effect on the financial statements is limited to contingent liabilities as a result of noncompliance (typically for fines, penalties, and interest), such a provision does not have a direct effect on determining financial statement amounts. Laws identified by the auditor that have a direct effect might include (1) new laws and regulations (not yet reflected on OMB's list) and (2) entity-specific laws and regulations. The concept of direct effect is discussed in AU 801 (SAS 74) and AU 317.

.04 In contrast, indirect laws relate more to the entity's operating aspects than to its financial and accounting aspects, and their financial statement effect is indirect. In other words, their effect may be limited to recording or disclosing liabilities <u>arising from noncompliance</u>. Examples of indirect laws and regulations include those related to environmental protection and occupational safety and health.

.05 The auditor is not responsible for testing compliance controls over or compliance with any <u>indirect</u> laws and regulations not otherwise identified by OMB or the entity (see paragraph 245.02.a.). However, as discussed in AU 317, the auditor should make inquiries of management regarding policies and procedures for the prevention of noncompliance with indirect laws and regulations. Unless possible instances of noncompliance with indirect laws or regulations come to the auditor's attention during the audit, no further procedures with respect to indirect laws and regulations are necessary.

.06 The auditor may elect to test compliance with indirect laws and regulations. For example, if the auditor becomes aware that the entity has operations similar to those of another entity that was recently in noncompliance with environmental laws and regulations, the auditor may elect to test compliance with such laws and regulations. The auditor may also elect to test provisions of direct laws and regulations that do not meet the materiality criteria in paragraph 245.02.b. but that are deemed significant, such as laws and regulations that have generated significant interest by the Congress, the media, or the public.

.07 The significant provisions identified by the above procedures are intended to include provisions of all laws and regulations that have a direct and material effect on the determining of financial statement amounts and therefore comply with GAGAS, AU 801 (SAS 74), and OMB audit guidance.

.08 In considering regulations to test for compliance, the auditor should consider externally imposed requirements issued pursuant to the Administrative Procedures Act, which has a defined due process. This would include regulations in the *Code of Federal Regulations*, but would not include OMB circulars and bulletins. Such circulars and bulletins generally implement laws, and the provisions of the laws themselves could be considered for compliance testing. Internal policies, manuals, and directives may be the basis for internal controls, but are not regulations to consider for testing for compliance.

250 - IDENTIFY RELEVANT BUDGET RESTRICTIONS

.01 To evaluate budget controls (see section 295 G) and to design compliance-related audit procedures relevant to budget restrictions, the auditor should understand the following information (which may be obtained from the entity or OGC):

- the Antideficiency Act (title 31 of the U.S. Code, sections 1341, 1342, 1349-1351, 1511-1519);
- the Purpose Statute (title 31 of the U.S. Code, section 1301);
- the Time Statute (title 31 of the U.S. Code, section 1502);
- OMB Circular A-34;
- title 7 of the GAO *Policy and Procedures Manual for Guidance of Federal Agencies*;
- the Impoundment Control Act; and
- the Federal Credit Reform Act of 1990.

.02 The auditor should read the following information relating to the entity's appropriation (or other budget authority) for the period of audit interest:

- authorizing legislation;
- enabling legislation and amendments;
- appropriation legislation and supplemental appropriation legislation;
- apportionments and budget execution reports (including OMB forms 132 and 133 and supporting documentation);
- Impoundment Control Act reports regarding rescissions and deferrals, if any;
- the system of funds control document approved by OMB; and
- any other information deemed by the auditor to be relevant to understanding the entity's budget authority, such as legislative history contained in committee reports or conference reports.

Although legislative histories are not legally binding, they may help the auditor understand the political environment surrounding the entity (i.e., why the entity has undertaken certain activities and the objectives of these activities).

.03 Through discussions with OGC and the entity and by using the above information, the auditor should identify all legally binding restrictions on the

entity's use of appropriated funds that are relevant to budget execution, such as restrictions on the amount, purpose, or timing of obligations and outlays ("relevant budget restrictions"). Additionally, the auditor should consider any legally binding restrictions that the entity has established in its fund control regulations, such as lowering the legally binding level for compliance with the Antideficiency Act to the allotment level.

.04 The auditor should obtain an understanding of the implications if the entity were to violate these relevant budget restrictions. In the internal control phase, the auditor identifies and tests the entity's controls to prevent or detect noncompliance with these relevant restrictions. The auditor may elect to evaluate controls over budget restrictions that are not legally binding but that may be considered sensitive or otherwise important.

.05 During these discussions with OGC and the entity, the auditor should determine whether any of these relevant budget restrictions relate to significant provisions of laws and regulations for purposes of testing compliance.

.06 For those entities that do not receive appropriated funds, the auditor should identify budget-related requirements that are legally binding on the entity. These requirements, if any, are usually found in the legislation that created the entity or its programs (such as the authorizing and enabling legislation) as well as any subsequent amendments. Although budget information on these entities may be included in the President's budget submitted to the Congress, this information usually is not legally binding. In general, certain budget-related restrictions (such as the Antideficiency Act) apply to government corporations but not to government-sponsored enterprises. Regardless, the auditor should consider the entity's budget formulation and execution as part of the control environment, as discussed in section 260.

260 – IDENTIFY RISK FACTORS

.01 The auditor's consideration of inherent risk, fraud risk, control environment, risk assessment, communication, and monitoring (parts of internal control) affects the nature, timing, and extent of substantive and control tests. This section describes (1) the impact of risk factors identified during this consideration on substantive and control tests, (2) the process for identifying these risk factors, and (3) the auditor's consideration of the entity's process for reporting under FMFIA (both for internal control (section 2 of FMFIA) and for financial management systems' conformance with system requirements (section 4 of FMFIA) and for formulating the budget.

IMPACT ON SUBSTANTIVE TESTING

.02 AU 312 provides guidance on the consideration of audit risk and defines "audit risk" as the risk that the auditor may unknowingly fail to appropriately modify an opinion on financial statements that are materially misstated. Audit risk can be thought of in terms of the following three component risks:

- **Inherent risk** is the susceptibility of an assertion to a material misstatement, assuming that there are no related internal controls.

- **Control risk** is the risk that a material misstatement that could occur in an assertion will not be prevented or detected and corrected on a timely basis by the entity's internal control. Internal control consists of five components: (1) the control environment, (2) risk assessment, (3) monitoring, (4) information and communication, and (5) control activities (defined in paragraph 260.08 below). This section will discuss the first three of the components and communication, which is part of the fourth component. Section 300 (Internal Control Phase) will discuss the information systems and control activities.

- **Detection risk** is the risk that the auditor will not detect a material misstatement that exists in an assertion.

AU 316 requires the auditor to consider fraud risk, which is a part of audit risk, making up a portion of inherent and control risk. Fraud risk consists of the risk of fraudulent financial reporting and the risk of misappropriation of assets that causes a material misstatement of the

financial statements. The auditor should specifically consider and document the risk of material misstatements of the financial statements due to fraud and keep in mind the consideration of fraud risk in designing audit procedures. Considering the risk of material fraud generally should be done concurrently with the consideration of inherent and control risk, but it should be a separate conclusion. The auditor also should consider the risk of fraud throughout the audit. Section 290 includes documentation requirements for the consideration of fraud risk.

.03 Based on the level of audit risk and an assessment of the entity's inherent and control risk, including the consideration of fraud risk, the auditor determines the nature, timing, and extent of substantive audit procedures necessary to achieve the resultant detection risk. For example, in response to a high level of inherent and control risk, the auditor may perform

- additional audit procedures that provide more competent evidential matter (nature of procedures);
- substantive tests at or closer to the financial statement date (timing of procedures); or
- more extensive substantive tests (extent of procedures), as discussed in section 295 E.

.04 Audit assurance is the complement of audit risk. The auditor can determine the level of audit assurance obtained by subtracting the audit risk from 1. (Assurance equals 1 minus risk).[1] AU 350.48 uses 5 percent as the allowable audit risk in explaining the audit risk model (95 percent audit assurance). The audit organization should determine the level of assurance to use, which may vary between audits based on risk. GAO auditors should use 95 percent. In other words, the GAO auditor, in order to provide an opinion, should design the audit to achieve at least 95 percent audit assurance that the financial statements are not materially misstated (5 percent audit risk). Section 470 provides guidance to the auditor on how to combine (1) the assessment of inherent and control risk (including fraud risk) and (2) substantive tests to achieve the audit assurance required by the audit organization.

---

[1] Assurance is not the same as statistical confidence. Assurance is a combination of quantitative measurement and auditor judgment.

.05 The auditor may consider it necessary to achieve increased audit assurance if the entity is politically sensitive or if the Congress has expressed concerns about the entity's financial reporting. In this case, the level of audit assurance should be approved by the Reviewer.

RELATIONSHIP TO CONTROL ASSESSMENT

.06 Internal control, as identified in AU 319 (SAS 55 amended by SAS 78), is a process—effected by an entity's governing body, management, and other personnel—designed to provide reasonable assurance regarding the achievement of objectives in the following categories (OMB audit guidance expands the category definitions as noted):[2]

- Reliability of **financial reporting**—transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements and RSSI in accordance with generally accepted accounting principles, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition. (Note that **safeguarding** controls (see paragraphs 310.02-.04) are considered as part of financial reporting controls, although they are also operations controls.)

- **Compliance** with applicable laws and regulations—transactions are executed in accordance with (a) laws governing the use of budget authority and other laws and regulations that could have a direct and material effect on the financial statements or RSSI, and (b) any other laws, regulations, and governmentwide policies identified by OMB in its audit guidance. (Note that **budget** controls are part of financial reporting controls as they relate to the statements of budgetary resources and of financing, but that they are also part of compliance controls in that they are used to manage and control the use of appropriated funds and other forms of budget authority in accordance with applicable law. These controls are described in more detail in section 295 G.)

- Effectiveness and efficiency of **operations**. These controls include policies and procedures to carry out organizational objectives, such as planning, productivity, programmatic, quality, economy, efficiency, and

[2] See also GAO's *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1, November 1999.

effectiveness objectives. Management uses these controls to provide reasonable assurance that the entity (1) achieves its mission, (2) maintains quality standards, and (3) does what management directs it to do. (Note that **performance measures** controls (those designed to provide reasonable assurance about reliability of performance reporting— transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management) are included in operations controls.)

.07 Some control policies and procedures belong in more than one category of control. For example, financial reporting controls include controls over the completeness and accuracy of inventory records. Such controls are also necessary to provide complete and accurate inventory records to allow management to analyze and monitor inventory levels to better control operations and make procurement decisions (operations controls).

.08 The five components of internal control relate to objectives that an entity strives to achieve in each of the three categories: financial reporting (including safeguarding), compliance, and operations (including performance measures) controls. The components are defined in AU 319 as:

- The **control environment** sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

- **Risk assessment** is the entity's identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.

- **Information and communication** are the identification, capture, and exchange of information in a form and time frame that enable employees to carry out their responsibilities.

- **Monitoring** is a process that assesses the quality of internal control performance over time.

- **Control activities** are the policies and procedures that help ensure that management directives are carried out.

PROCESS FOR IDENTIFYING RISK FACTORS

.09 In the planning phase, the auditor should (1) identify conditions that significantly increase inherent, fraud, and control risk (based on identified control environment, risk assessment, communication, or monitoring weaknesses) and (2) conclude whether any identified control risks preclude the effectiveness of specific control activities in significant applications. The auditor identifies specific inherent risks, fraud risks, and control environment, risk assessment, communication, and monitoring weaknesses based on information obtained earlier in the planning phase, primarily from understanding the entity's operations and preliminary analytical procedures. The auditor considers factors such as those listed in paragraphs 260.16-.61 in identifying such risks and weaknesses. These factors are general in nature and require the auditor's judgment in determining (1) the extent of procedures (testing) to identify the risks and weaknesses and (2) the impact of such risks and weaknesses on the entity and its financial statements. Because this risk consideration requires the exercise of significant audit judgment, it should be performed by experienced audit team personnel.

.10 The auditor considers the implications of these risk factors on related operations controls. For example, inherent risk may be associated with a material liability for loan guarantees because it is subject to significant management judgment. In light of this inherent risk, the entity should have strong operations controls to monitor the entity's exposure to losses from loan guarantees. Potential weaknesses in such operations controls could significantly affect the ultimate program cost. Therefore, the need for operations controls in a particular area or the awareness of operations control weaknesses related to these risk factors should be identified and considered for further review, as discussed in section 275.

.11 Specific conditions that may indicate inherent or fraud risks or control environment, risk assessment, communication, or monitoring weaknesses are provided in sections 295 A and 295 B, respectively. These sections are designed to aid the auditor in identifying these risks and weaknesses but are not intended to be all inclusive. The auditor should consider any other factors and conditions deemed relevant.

.12 The auditor identifies and documents any significant risk factors after considering (1) his/her knowledge of the entity (obtained in previous steps in the planning phase); (2) the risk factors discussed in paragraphs 260.16-.61

and in sections 295 A and 295 B; and (3) other relevant factors. These risks and weaknesses and their impact on proposed audit procedures should be documented on the General Risk Analysis (GRA) or equivalent (see section 290). The auditor also should summarize and document any account-specific risks on the Account Risk Analysis (ARA) or equivalent (see sections 290 and 395 I).

.13 For each risk factor identified, the auditor documents the nature and extent of the risk or weakness; the condition(s) that gave rise to that risk or weakness; and the specific cycles, accounts, line items, and related assertions affected (if not pervasive). For example, the auditor may identify a significant risk that the valuation of the net receivables line item could contain a material misstatement due to (1) the materiality of the receivables and potential allowance, (2) the subjectivity of management's judgment related to the loss allowance (inherent risk), and (3) management's history of aggressively challenging any proposed adjustments to the valuation of the receivables (control environment weakness). The auditor should also document other considerations that may mitigate the effects of identified risks and weaknesses. For example, the use of a lock box (a control activity) may mitigate inherent risks associated with the completeness of cash receipts.

.14 The auditor also should document, in the GRA or equivalent, the overall effectiveness of the control environment, risk assessment, communication, and monitoring, including whether weaknesses preclude the effectiveness of specific control activities. The focus should be on management's overall attitude, awareness, and actions, rather than on specific conditions related to a control environment, risk assessment, communication, or monitoring factor. This assessment will be considered when determining the control risk associated with the entity.

.15 In assessing the control environment, risk assessment, communication, and monitoring, the auditor should specifically assess the quality of the entity's process for compliance with FMFIA (see paragraphs 260.53-.57) and should obtain an overall understanding of the budget formulation process (see paragraph 260.61).

INHERENT RISK FACTORS

.16 Inherent risk factors incorporate characteristics of an entity, a transaction, or account that exist due to

- the nature of the entity's programs,
- the prior history of audit adjustments, or
- the nature of material transactions and accounts.

The assessment of inherent risk generally should be limited to significant programs, transactions, or accounts. For each factor listed below, section 295 A lists conditions that may indicate inherent risk.

a. **Nature of the entity's programs:** The mission/business of an entity includes the implementation of various programs or services. The characteristics of these programs or services affect the entity's susceptibility to errors and fraud and sensitivity to changes in economic conditions. For example, student loan guarantee programs may be more susceptible to errors and fraud because of loans issued and serviced by third parties.

b. **Prior history of significant audit adjustments:** Significant audit adjustments identified in previous financial statement audits or other audits often identify problem areas that may result in financial statement misstatements. For example, the prior year's audit may have identified the necessity for recording a contingent liability as the result of certain economic conditions. The auditor could then focus on

   - determining whether similar conditions continue to exist;
   - understanding management's response to such conditions (including implementation of controls), if any; and
   - assessing the nature and extent of the related inherent risk.

c. **Nature of material transactions and accounts:** The nature of an entity's transactions and accounts has a direct relation to the risk of errors or fraud. For example, accounts involving subjective management judgments, such as loss allowances, are usually of higher risk than those involving objective determinations.

INFORMATION SYSTEMS (IS) EFFECTS ON INHERENT RISK

.17 Information systems (IS) do not affect the audit objectives for an account or a cycle. However, IS can introduce inherent risk factors not present in a manual accounting system. The auditor should (1) consider each of the following IS factors and (2) assess the overall impact of IS processing on inherent risk. The impact of these factors typically will be pervasive in nature. An IS auditor may assist the auditor in considering these factors and making this assessment. More detail on assessing IS controls in a financial statement audit is available in FISCAM, and a flowchart of the steps to follow is in section 295 J.

a. **Uniform processing of transactions:** Because IS process groups of identical transactions consistently, any misstatements arising from erroneous computer programming will occur consistently in similar transactions. However, the possibility of random processing errors is reduced substantially in computer-based information systems.

b. **Automatic processing:** The information system may automatically initiate transactions or perform processing functions. Evidence of these processing steps (and any related controls) may or may not be visible.

c. **Increased potential for undetected misstatements:** Computers use and store information in electronic form and require less human involvement in processing. This increases the potential for individuals to gain unauthorized access to sensitive information and to alter data without visible evidence. Due to the electronic form, changes to computer programs and data are not readily detectible. Also, users may be less likely to challenge the reliability of computer output than manual reports.

d. **Existence, completeness, and volume of the audit trail:** The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. For example, the audit trail for a purchase could include a purchase order, a receiving report, an invoice, invoice register (purchases summarized by day, month, and/or account), and general ledger postings from the invoice register. Some computerized financial management systems are designed so that the audit trail exists for only a short period (such as in on-line systems), only in an electronic format, or only in summary form. Also, the information

generated may be too voluminous to allow effective manual review. For example, one posting to the general ledger may result from the computer summarization of information from hundreds of locations.

e. **Nature of the hardware and software used in IS:** The nature of the hardware and software can affect inherent risk, as illustrated below:

- The type of computer processing (on-line, batch-oriented, or distributed) presents different levels of inherent risk. For example, the inherent risk of unauthorized transactions and data entry errors may be greater for on-line processing than for batch-oriented processing.

- Peripheral access devices or system interfaces can increase inherent risk. For example, Internet and dial-up access to a system increases the system's accessibility to additional persons and therefore increases the risk of unauthorized access to computer resources.

- Distributed networks enable multiple computer processing units to communicate with each other, increasing the risk of unauthorized access to computer resources and possible data alteration. On the other hand, distributed networks may decrease the risk of conflicting computerized data between multiple processing units.

- Applications software developed in-house may have higher inherent risk than vendor-supplied software that has been thoroughly tested and is in general commercial use.

f. **Unusual or nonroutine transactions:** As with manual systems, unusual or nonroutine transactions increase inherent risk. Programs developed to process such transactions may not be subject to the same procedures as programs developed to process routine transactions. For example, the entity may use a utility program to extract specified information in support of a nonroutine management decision.

FRAUD RISKS

.18 The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Accordingly, the auditor is concerned with the **risk of material misstatement due to fraud (fraud risk)**. The primary factor that distinguishes fraud from error is that the action causing the misstatement in fraud is intentional. (See section 230 related to materiality, including quantitative and qualitative considerations.)

.19 Two types of misstatements are relevant to the auditor's consideration of fraud in an audit of financial statements—misstatements arising from fraudulent financial reporting and misstatements arising from misappropriation of assets. **Misstatements arising from fraudulent financial reporting** are intentional misstatements or omissions of amounts or disclosures in financial statements to deceive financial statement users. They could involve intentional alteration of accounting records, misrepresentation of transactions, intentional misapplication of accounting principles, or other means. **Misstatements arising from misappropriation of assets** involve theft of an entity's assets that result in misstatements in the financial statements. They could involve theft of property, embezzlement of receipts, fraudulent payments, or other means. (See section 310 for internal control over safeguarding assets. Safeguarding controls relate to protecting assets against loss from unauthorized acquisition, use, or disposition.)

.20 In considering misstatements arising from misappropriation of assets, the auditor should consider fraud risks associated with improper payments. Some of the improper payments made by federal government entities could involve fraud. The Improper Payments Information Act of 2002 (P.L. 107-300) defines improper payments as any payment that should not have been made or that was made in an incorrect amount (including overpayments and underpayments) under statutory, contractual, administrative, or other legally applicable requirements. The act requires agency heads to annually review all programs and activities that they administer, identify those that might be susceptible to significant improper payments,[1] estimate annual improper payments for those identified programs, and—for programs for which estimated improper payments exceed $10 million—report certain information to the Congress. Although the act has this reporting threshold, the auditor might consider improper payments amounting to $10 million or less quantitatively or qualitatively material.

.21 As discussed in paragraph .18, the auditor is responsible for obtaining reasonable, but not absolute, assurance about whether the financial statements are free of material misstatement. Absolute assurance cannot be attained, and the auditor's report does not provide absolute assurance. A properly planned and performed audit might not detect a material misstatement, and the subsequent discovery of a material misstatement does not, in and of itself, provide evidence that the auditor did not conform with auditing standards.

---

[1] Agencies first need to determine which programs and activities are susceptible (at high risk) to improper payments. In determining this, OMB has issued guidance defining significant improper payments as those that exceed both 2.5 percent of program payments and $10 million. See OMB Memorandum M-03-13, *Improper Payments Information Act of 2002, Public Law 107-300* (May 21, 2003).

.22 In addition, the auditor should be alert to situations or transactions that could be indicative of abuse. Abuse is distinct from fraud and illegal acts. Abuse involves behavior that is deficient or improper (but not necessarily fraudulent or illegal) when compared with behavior that a prudent person would consider reasonable and necessary business practice given the facts and circumstances. The auditor is not required to detect abuse. However, if indications of abuse that could result in material misstatement of the financial statements or other financial data come to the auditor's attention, the auditor should apply audit procedures specifically directed to determine whether abuse has occurred and the effect, if any, on the financial statements. The auditor should consider both quantitative and qualitative factors in making judgments about the materiality of possible abuse and about related audit procedures. The determination of abuse is subjective, and the auditor does not provide reasonable assurance of detecting abuse. (See GAGAS, paragraphs 4.19-.20.)

Characteristics of Fraud

.23 Three conditions generally are present when fraud occurs:

- **Incentive/Pressure**—Management, other employees, or external parties (for example, for some improper payments) have an incentive or are under pressure, which provides a motive to commit fraud.

- **Opportunity**—Circumstances exist, such as the absence of controls, ineffective controls, or the ability of management to override controls, that provide an opportunity to commit fraud.

- **Attitude/Rationalization**—Individuals involved are able to rationalize committing fraud. Some individuals possess an attitude, character, or ethical values that allow them to knowingly and intentionally commit a dishonest act.

Generally, the greater the incentive or pressure, the more likely an individual will be able to rationalize the acceptability of committing fraud.

.24 Management is in a position that could permit it to perpetrate fraud by directly or indirectly manipulating accounting records; overriding controls, sometimes in unpredictable ways; or committing other fraudulent or improper acts.

Fraud Risk Factors

.25 Although fraud is usually concealed, the presence of **fraud risk factors** that indicate incentive/pressure, opportunity, or attitude/rationalization might alert the auditor to a significant risk of fraud. However, fraud risk factors do not necessarily indicate that fraud exists. Examples of fraud risk factors, classified by the two types of fraudulent misstatements and then by these three conditions, include the following:

a. **Examples** related to misstatements arising from fraudulent financial reporting:

- Incentive/Pressure—Incentive exists for management to report reduced program costs or costs that are consistent with budgeted amounts, or excessive pressure exists to meet unrealistic deadlines or other requirements.

- Opportunity—Key financial statement amounts are based on significant estimates that involve subjective judgments or uncertainties that are difficult to corroborate, or management is in a position to override controls for processing adjustments or unusual transactions.

- Attitude/Rationalization— Employees perceive that penalties exist for reporting honest results, or employees consider requirements such as performance targets unrealistic.

b. **Examples** related to misstatements arising from misappropriation of assets:

- Incentive/Pressure—Employees who are disgruntled because of impending layoffs have an incentive to misappropriate assets, or pressure to meet programmatic objectives such as for rapid benefit payments increases the risk of fraudulent improper payments.

- Opportunity—Employees have access to assets that are small in size and valuable or the authority to disburse funds, or a program has weaknesses in internal control related to fraudulent improper payments.

- Attitude/Rationalization—Employees believe that management is unethical, or individuals believe they are entitled to the entity's assets.

Fraud risk factors represent inherent or control risk factors. As discussed in paragraph .02, the auditor should consider fraud risk factors in assessing inherent and control risk. Sections 295A and 295B include additional examples of fraud risk factors.

Professional Skepticism

.26 The auditor should exercise professional skepticism—an attitude that includes a questioning mind and a critical assessment of audit evidence—throughout the audit. The auditor should maintain a mindset that recognizes the possibility that a material misstatement due to fraud might be present, regardless of any past experience with the entity and regardless of the auditor's belief about management's honesty and integrity.

Brainstorming Meeting(s) about Potential Fraud Risks

.27 Audit team members should exchange ideas in one or more "brainstorming" meeting(s) to identify potential fraud risks. They should discuss how and where the financial statements could be susceptible to material fraudulent misstatement, how management could perpetrate and conceal fraudulent financial reporting, how assets could be misappropriated (including through fraudulent improper payments), how management could override controls, and how the auditor might respond to these risks. They also should consider known internal and external fraud risk factors (including any related to fraudulent improper payments) and categorize these factors by type of misstatement and by incentive/pressure, opportunity, and attitude/rationalization. The brainstorming discussion should emphasize the need to exercise professional skepticism in gathering and evaluating evidence throughout the audit.

.28 The Audit Director, Assistant Director, and all other team members who have significant responsibilities in planning and performing the audit should participate in brainstorming, which may be performed in a single meeting or in multiple meetings. While different members may participate in different meetings, each brainstorming meeting should include at least one experienced team member, and all team members should be familiar with the collective results of the brainstorming meeting(s). Determining the brainstorming participants (for example, it might be useful to include stakeholders and specialists, such as IS auditors) and the number of brainstorming meeting(s) are matters of auditor judgment.

.29 The auditor's consideration of fraud risks should be ongoing throughout the audit. Near the completion of fieldwork, the auditor should evaluate whether the audit test results indicate the need for a change in the assessment of the fraud risks made earlier or the need for additional or different audit procedures (see paragraphs 540.18-.19). Accordingly, communications with the audit team members about fraud should occur as needed throughout the audit, and the auditor may hold multiple, periodic brainstorming meetings.

Information to Identify Fraud Risks

.30 Fraud risks might be identified as a result of replies to inquiries. To obtain information about fraud risks, the auditor should inquire of management about:

- any knowledge of fraud or suspected fraud (including fraudulent improper payments), or related allegations;
- management's understanding of fraud risks, including any specific risks the entity has identified and any account balances or classes of transactions having likely fraud risks (including information about any fraudulent improper payments that the agency identified in making assessments related to the Improper Payments Information Act of 2002);
- any antifraud programs and controls the entity has established;[2]
- the nature and extent that locations or business segments, if any, are monitored, and whether there are particular locations or segments for which fraud risks might be more likely;
- whether and how management communicates to employees its views on business practices and ethical behavior; and
- whether management has reported to the audit committee (referred to as "financial management advisory committee" in some federal entities) or others with equivalent authority and responsibility on how the entity's internal control prevents, deters, or detects fraud.

.31 In addition to inquiring of management, inquiring of others might provide a different perspective or provide other important information. Accordingly, the auditor should perform the following inquiries and related procedures:

a. Obtain information about instances of fraud (including any related to fraudulent improper payments) reported by the inspector general, ordinarily by asking the Special Investigator Unit to summarize how cases of reported fraud were committed, and then ask management or the Office of Inspector General whether related controls have been strengthened.

b. Inquire of the audit committee or others with equivalent authority and responsibility about fraud risks and any fraud or suspected fraud, and obtain an understanding of how they exercise oversight.

[2] An example document, *Management Antifraud Programs and Controls*, commissioned by the Fraud Task Force of the Auditing Standards Board of the AICPA, is available at the AICPA's web site, www.aicpa.org.

c. Inquire of internal audit personnel about fraud risks, any procedures to detect fraud during the reporting period, management's response to any such findings, and any fraud or suspected fraud.

d. Inquire of other personnel about fraud or suspected fraud. The auditor should use judgment to determine whom to ask and the extent of inquiries. For example, the auditor may make inquiries of employees with varying levels of authority, operating personnel not directly involved in the financial reporting process, employees familiar with complex or unusual transactions or with improper payments, and in-house legal counsel.

e. If inconsistencies arise from the auditor's inquiries of management and others, obtain additional evidence to resolve the inconsistencies.

.32 The auditor also should perform the following procedures:

a. Obtain and review the agency's (1) plan to identify improper payments and (2) report, if any, on improper payments (or information about any findings) that resulted from the agency's review under the Improper Payments Information Act of 2002.

b. Determine whether preliminary analytical procedures disclosed any unusual or unexpected relationships that might indicate fraud risks. Where revenue is (or is expected to be) material, analytical procedures should include those related to revenue—for example, trend analysis—to identify unusual or unexpected relationships that might indicate fraudulent financial reporting of revenue (see section 225 related to preliminary analytical procedures).

c. Consider whether any fraud risk factors exist (see paragraph .25).

d. Consider other information that might help identify fraud risks, such as information that resulted from previous audits, the brainstorming meeting(s), procedures related to accepting and continuing engagements, any reports on interim financial statements, and inherent risks identified at the account or transaction level.

Identification and Assessment of Fraud Risks

.33 To identify fraud risks (including any related to fraudulent improper payments), the auditor should perform the following procedures:

a. Evaluate the information obtained in the procedures described in paragraphs .28-.32, in the context of the three conditions that generally are present when fraud occurs— incentive/pressure, opportunity, and attitude/rationalization. While fraud risk might be greatest when all three of these conditions are evident, observation of one or more of these conditions might indicate a fraud risk.

b. Where revenue is (or is expected to be) material, evaluate whether there are fraud risks related to revenue recognition (for example, through premature recognition or fictitious revenue). If the auditor concludes that improper revenue recognition does not represent a fraud risk, the auditor should document the reasons supporting that conclusion (see paragraph 290.04 h).

c. Evaluate the possibility that management could override controls, even if specific fraud risks have not been identified.

.34 For each identified fraud risk, the auditor should determine whether it relates to (1) specific financial statement account balances or classes of transactions and related assertions or (2) more pervasively to the financial statements as a whole. Generally, relating fraud risks to the individual accounts, classes of transactions, and assertions helps in designing audit procedures in response to these risks.

.35 As part of understanding internal control sufficient to plan the audit, the auditor should (1) evaluate whether programs and controls that address identified fraud risks have been suitably designed and placed in operation and (2) determine whether these programs and controls mitigate these risks or whether specific control deficiencies exacerbate these risks. See section 350 regarding testing the operating effectiveness of controls that are determined to mitigate these risks.

.36 The auditor should assess the identified fraud risks, taking into consideration the results of the procedures described in the preceding paragraph. In making this assessment, using professional judgment, the auditor should consider all significant aspects of each of these risks , including the type of misstatement, the significance and pervasiveness of the risk, and the likelihood that it could result in a material misstatement.

Response to Assessed Fraud Risks

.37 The auditor must respond to the assessed risks of material misstatement due to fraud. The nature and significance of these fraud risks, as well as programs and controls that address identified fraud risks, influence the auditor’s response. The auditor should use professional judgment in determining the appropriate

response for the circumstances and exercise professional skepticism in gathering and evaluating audit evidence. The response should (1) have an overall effect on the conduct of the audit (see paragraph .39), (2) address fraud risks that relate to management override of controls (see paragraph .40), and, (3) for any of these risks that relate to specific financial statement account balances or classes of transactions and related assertions, involve the nature, timing, and extent of audit procedures (see paragraph .41). If it is not practicable, as part of a financial statement audit, to design audit procedures that sufficiently respond to the fraud risks, the auditor should consider requesting assistance from the Special Investigator Unit.

.38 In some instances, the audit plan could, for reasons other than responding to fraud risk, include procedures and personnel and supervisory assignments that are sufficient to respond to a fraud risk. In these instances, the auditor may conclude that no further response is required. For example, with respect to timing, audit procedures could be planned as of the date that the reporting period ends, both as a response to a fraud risk and for other reasons.

.39 The auditor should respond to the fraud risks in ways that have an overall effect on the conduct of the audit, as follows:

a. **Assignment of personnel and supervision**—Assign audit team staffing and/or supervision so that the knowledge, skill, and ability of personnel assigned significant responsibilities are commensurate with the auditor's assessment of the fraud risks—for example, the auditor may assign a fraud specialist or more experienced personnel or may increase supervision in response to identified fraud risks (also see section 270 related to IS auditors).

b. **Review of accounting principles**—Review management's selection and collective application of significant accounting principles, particularly those related to subjective measurements and complex transactions.

c. **Unpredictability of audit procedures**—Incorporate an element of unpredictability in the selection of audit procedures from reporting period to reporting period—for example, perform substantive tests of selected account balances and assertions not otherwise tested due to their materiality and risk, adjust the timing of audit tests, use a different method to select items for testing, or perform procedures at different locations or at locations on an unannounced basis. Statistical sampling selection usually provides an element of unpredictability as to the specific items tested (see section 480). Generally, the auditor should not inform entity personnel of specific audit procedures prior to performing them.

.40 The auditor should perform the following procedures to specifically address the risk that management can perpetrate fraud by overriding controls:

a. **Examination of journal entries and other adjustments**—Examine journal entries and other adjustments for evidence of possible material misstatement due to fraud. These include reclassifications, consolidating entries, and other routine and nonroutine journal entries and adjustments. The auditor should obtain an understanding of the financial reporting process and the controls over journal entries and other adjustments; identify and select journal entries and other adjustments for testing; determine the nature, timing, and extent of the testing (ordinarily including tests of journal entries and other adjustments at the end of the reporting period); and inquire of individuals involved in the financial reporting process about inappropriate or unusual activity related to the processing of journal entries and other adjustments.

b. **Review of accounting estimates**—Review accounting estimates for biases that could result in material misstatement due to fraud. In preparing financial statements, management is responsible for making judgments or assumptions that affect significant accounting estimates and for monitoring the reasonableness of these estimates on an ongoing basis. The auditor should consider whether differences between (1) estimates best supported by the evidence and (2) the estimates included in the financial statements, even if the estimates are individually reasonable, indicate possible bias by management, in which case the auditor should reconsider the estimates taken as a whole. The auditor also should perform a retrospective review of significant accounting estimates used in the prior year's financial statements, focusing on sensitive or subjective aspects, to determine whether they indicate possible bias by management. Further, the auditor should be alert for aggressive or inconsistently applied estimates.

c. **Evaluation of business rationale for significant unusual transactions**—Evaluate the business rationale for any significant unusual transactions, considering whether (1) the form of these transactions is overly complex, (2) management has discussed the nature of and accounting for these transactions with the audit committee or others with equivalent authority and responsibility or the board of directors, if any, (3) management is placing more emphasis on particular accounting treatments than on the underlying economics of the transactions, (4) transactions that involve related parties have been properly reviewed and approved by the audit committee or others with equivalent authority and responsibility or the board of directors, if any, and (5) the transactions involve previously unidentified related parties (see

section 902) or related parties that do not have the substance or financial strength to support the transaction without assistance from the entity.

.41 For fraud risks related to specific financial statement account balances or classes of transactions and related assertions, the specific response will depend on the types of risks and the specific balances or classes and assertions, but it generally should involve both substantive and control tests. The response should involve the following:

a. **Nature** of audit procedures—for example, obtaining related evidence from independent external sources rather than internal sources;

b. **Timing** of audit procedures—for example, performing substantive testing at or near the end of the reporting period rather than at an interim date; and

c. **Extent** of audit procedures—for example, increasing audit sample sizes.

Section 295 I provides additional examples of responses.

CONTROL ENVIRONMENT FACTORS

.42 As discussed in AU 319 (SAS 55 amended by SAS 78), control environment risk factors incorporate management's attitude, awareness, and actions concerning the entity's control environment. These factors include

- integrity and ethical values,
- commitment to competence,
- management's philosophy and operating style,
- organizational structure,
- assignment of authority and responsibility,
- human resource policies and practices,
- management's control methods over budget formulation and execution,
- management's control methods over compliance with laws and regulations, and
- the functioning of oversight bodies (including congressional committees).

.43 The auditor should obtain sufficient knowledge of the control environment to determine whether the collective effect of these factors establishes, enhances, or mitigates the effectiveness of specific control activities. In making this determination, the auditor should consider the following factors and their effect on internal control. For each factor listed below, section 295 B lists conditions that may indicate control environment weaknesses.

a. **Integrity and ethical values:** Control effectiveness cannot rise above the integrity and ethical values of those who create, administer, and monitor the controls. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of the other components. Integrity and ethical behavior result when the entity and its leaders have high ethical and behavioral standards and properly communicate them and reinforce them in practice. The standards include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. The communication of

entity values and behavioral standards to personnel takes place through policy statements and codes of conduct and by example.

b. **Commitment to competence:** Competence is the knowledge and skills necessary to accomplish tasks required by an individual's job. Commitment to competence includes management's consideration of the competence levels for various jobs and the requisite skills and knowledge.

c. **Management's philosophy and operating style:** Management's philosophy and operating style encompass a broad range of beliefs, concepts, and attitudes. Such characteristics may include management's approach to taking and monitoring operational/program risks, attitudes and actions toward financial reporting, emphasis on meeting financial and operating goals, and management's attitude toward information processing, accounting, and personnel.

d. **Organizational structure:** An entity's organizational structure provides the overall framework for planning, directing, and controlling operations. The organizational structure should appropriately assign authority and responsibility within the entity. An organizational structure includes the form and nature of an entity's organizational units, including the data processing organization, and related management functions and reporting relationships.

e. **Assignment of authority and responsibility:** An entity's policies or procedures for assigning authority for operating activities and for delegating responsibility affect the understanding of established reporting relationships and responsibilities. This factor includes policies relating to appropriate business practices, knowledge and experience of key personnel, and resource allocations. It also includes policies and communications to ensure that all personnel understand the entity's objectives, how they contribute to these objectives, and how and for what they will be held accountable.

f. **Human resource policies and practices:** Human resource policies and practices affect an entity's ability to employ sufficient competent and trustworthy personnel to accomplish its goals and objectives. Such policies and practices include hiring, training, evaluating, promoting, compensating, and assisting employees in the performance of their assigned responsibilities by giving them the necessary resources.

g. **Management's control methods over budget formulation and execution:** Management's budget control methods affect the authorized use of appropriated funds. Budget formulation is discussed in more detail in paragraph 260.61, and controls over budget execution (budget controls) are addressed in more detail in section 300.

h. **Management's control methods over compliance with laws and regulations:** Such methods have a direct impact on an entity's compliance with applicable laws and regulations. (Compliance controls are addressed in more detail in section 300).

i. **The functioning of oversight groups:** An entity's oversight groups typically are responsible for overseeing both business activities and financial reporting. The effectiveness of an oversight group is influenced by its authority and its role in overseeing the entity's business activities. In the federal government, oversight groups are the Congress and the central agencies (OMB, Treasury, GSA, OPM, and GAO). Within agencies, senior management councils may also have a role in overseeing operations and programs.

RISK ASSESSMENT FACTORS

.44 Risk assessment is an entity's internal process for identifying, analyzing, and managing risks relevant to achieving the objectives of reliable financial reporting, safeguarding of assets, and compliance with budget and other laws and regulations. For example, risk assessment may address how the entity analyzes significant estimates recorded in the financial statements or how it considers the possibility of unrecorded transactions. Risks can arise due to both internal and external circumstances such as:

- changes in the operating or statutory environment,
- new personnel who may have a different focus on internal control,
- new or significantly changed information systems,
- rapid growth of programs which can strain controls,
- new technology which may change risks,
- new programs or activities which may introduce new control risks,
- restructurings or budget cutbacks which may include downsizing and changes in supervision and segregation of duties, or

- adoption of new accounting principles which may affect risks in preparing financial statements.

.45 The auditor should gain sufficient knowledge of the entity's risk assessment process to understand how management considers risks relevant to the objectives of financial reporting (including safeguarding), and compliance with budget and other laws and decides what actions to take. This understanding may include how management identifies risks, estimates their significance, assesses the likelihood of occurrence, and relates them to financial reporting.

COMMUNICATION FACTORS

.46 Communication involves providing an understanding of individual roles and responsibilities pertaining to internal control. It includes the extent to which personnel understand how their activities relate to the work of others and the means of reporting exceptions to an appropriate higher level within the entity. Open communication channels help ensure that exceptions are reported and acted on. Communication takes such forms as policy manuals, accounting and financial reporting manuals, and memoranda. Communication also may be electronic, oral, and through the actions of management in demonstrating acceptable behavior.

.47 The auditor should obtain sufficient knowledge of the means the entity uses to communicate roles and responsibilities for, and significant matters relating to financial reporting, safeguarding, and compliance with budget and other laws and regulations.

MONITORING FACTORS

.48 Monitoring is the process by which management assesses the quality of internal control performance over time. This may include ongoing activities, such as regular management and supervision, or communications from external parties, such as customer complaints or regulator comments that may indicate areas in need of improvement. This also may include separate evaluations, such as FMFIA work and IG or internal auditor work, or a combination of ongoing activities and separate evaluations.

.49 The auditor should gain sufficient knowledge of the major types of activities the entity uses to monitor internal control over financial reporting, including

safeguarding, and compliance with budget and other laws and regulations and how those activities are used to initiate corrective actions.

.50 The IG's office or internal audit is often an important part of monitoring. The IG's office is responsible for (1) conducting and supervising audits and investigations relating to programs and operations, (2) providing leadership and coordination, including recommending policies for programs and operations, and (3) keeping the entity head and the Congress informed about problems and deficiencies, including the progress of corrective actions. The auditor should assess the effectiveness of the IG or internal audit as a monitoring control. However, if the auditor is the IG, the office should not attempt to assess its effectiveness as a control. Evaluating an IG's office or internal audit includes consideration of its authority and reporting relationships, the qualifications of its staff, and its resources. (In using the work of the IG or internal auditors, refer to section 650.)

IS EFFECTS ON THE CONTROL ENVIRONMENT, RISK ASSESSMENT, COMMUNICATION, AND MONITORING

.51 IS affects the effectiveness of the control environment, risk assessment, communication, and monitoring. For example, controls that normally would be performed by separate individuals in manual systems may be concentrated in one computer application and pose a potential segregation-of-duties problem.

.52 The auditor should consider the following IS factors in making an overall assessment of the control environment, risk assessment, communication, and monitoring. An IS auditor may assist the auditor in considering these factors:

a. **Management's attitudes and awareness with respect to IS:** Management's interest in and awareness of IS functions is important in establishing an organizationwide consciousness of control issues. Management may demonstrate such interest and awareness by

- considering the risks and benefits of computer applications;
- communicating policies regarding IS functions and responsibilities;
- overseeing policies and procedures for developing, modifying, maintaining, and using computers and for controlling access to programs and files;

- considering the inherent and control risk, including fraud risk, related to IS;
- responding to previous recommendations or concerns;
- quickly and effectively planning for, and responding to, computerized processing crises; and
- depending on computer-generated information for key operating decisions.

b. **Organization and structure of the IS function:** The organizational structure affects the control environment. Centralized structures often have a single computer processing organization and use a single set of system and applications software, enabling tighter management control over IS. In decentralized structures, each computer center generally has its own computer processing organization, application programs, and system software, which may result in differences in policies and procedures and various levels of compliance at each location.

c. **Clearly defined assignment of responsibilities and authority:** Appropriate assignment of responsibility according to typical IS functional areas can affect the control environment. Factors to consider include

- how the position of the Chief Information Officer (CIO) fits into the organizational structure;
- whether duties are appropriately segregated within the IS function, since lack of segregation typically affects all systems;
- the extent to which management external to the IS function is involved in major systems development decisions; and
- the extent to which policies, standards, and procedures are documented, understood, followed, and enforced.

d. **Management's ability to identify and to respond to potential risk:** Computer processing, by its nature, introduces additional risk factors. The entity should be aware of these risks and should develop appropriate policies and procedures to respond to any IS issues that might occur. Factors to consider include

- the methods for monitoring incompatible functions and for enforcing segregation of duties and

- management's mechanism for identifying and responding to unusual or exceptional conditions.

FEDERAL MANAGERS' FINANCIAL INTEGRITY ACT OF 1982

.53 In considering the control environment, risk assessment, communication, and monitoring, the auditor should assess the quality of the FMFIA process to provide evidence of management's control consciousness and the overall quality of the control environment, risk assessment, communication, and monitoring. In this regard, the quality of the FMFIA process is a good indicator of management's (1) philosophy and operating style, (2) assignment of authority and responsibility, and (3) control methods for monitoring and follow-up. The FMFIA process also may be the basis for management's assertion about the effectiveness of internal control (section 2) and about the entity's financial management systems' substantial compliance with FFMIA requirements (section 4).

.54 In considering the quality of the FMFIA process, the auditor generally should perform the following procedures. If the entity does not issue its own FMFIA report, the auditor should perform the following with respect to information the entity contributes to the FMFIA report in which the entity is included.

- Read
  - the FMFIA report,
  - important workpapers prepared by the entity in support of the FMFIA report,
  - IG reports on FMFIA compliance,
  - OMB's most recent annual letter concerning FMFIA reporting, and
  - management's description of the FMFIA process.

- Discuss the FMFIA process with appropriate entity management (including management's opinion of the quality of the process).

- Understand
  - how the FMFIA process is organized;
  - who is assigned to manage the process, including the staffing level, experience and qualifications of assigned personnel, and reporting responsibilities; and
  - how the process finds and evaluates weaknesses.

- Identify the entity's actions on previously reported weaknesses and examine agency documentation that demonstrates the results/effectiveness of those actions.

- Determine whether the audit finds different issues from those identified in the FMFIA process. (If so, see section 580 for reporting on FMFIA.)

.55 In assessing the quality of the FMFIA process, the auditor should consider whether management procedures and supporting documentation are sufficient to (1) provide management with reasonable assurance that FMFIA objectives have been achieved and (2) meet OMB requirements. This assessment is based on the auditor's overview and is not a result of extensive tests. Factors for the auditor to consider may include

- evidence of efforts to rectify previously identified material weaknesses;
- management's commitment of resources to the FMFIA process, as reflected in the skills, objectivity, and number of personnel assigned to manage the process;
- extent to which management's methodology and assessment process conform to the guidance in Circulars A-123 (June 21, 1995) and A-127 (July 23, 1993 and revisions in Transmittal Memorandum No. 2, dated June 10, 1999) and related OMB guidelines;
- IG and internal auditor involvement (if any);
- the process used to identify and screen material weaknesses as FMFIA reports are consolidated and moved up the entity's hierarchy; and
- the sources that identify material weaknesses, since items identified by management personnel, rather than from IG, GAO, or other external reports, demonstrate that the process can detect and report weaknesses.

.56 The auditor's assessment of the quality of the FMFIA process will affect the auditor's ability to use information in the FMFIA report and supporting documentation when identifying risks, testing controls, and preparing workpapers. The higher the quality of the FMFIA process, the more likely the auditor will be able to use the FMFIA findings in the financial audit. The auditor should document the assessment of the quality of the FMFIA

process in the audit workpapers. Regardless, any material weaknesses identified in the FMFIA report should be considered in considering risk.

.57 The reliance that the auditor places on management's FMFIA work depends on a number of factors as discussed in FAM 650.

Federal Financial Management Improvement Act of 1996

.58 As part of its FMFIA work, management determines whether its financial management systems comply with the requirements found in OMB Circular A-127, *Financial Management Systems*. Under FFMIA, the auditor is required to report whether the financial management systems' substantially comply with those requirements. Further, OMB issues guidance that agencies and auditors should consider when addressing compliance with FFMIA.

.59 During the planning phase, the auditor generally should understand what management did to determine that the entity's systems were in substantial compliance in order to report under FMFIA. The entity may have used the OMB FFMIA guidance, the GAO Financial Management Series of checklists for Systems Reviewed Under the Federal Financial Management Improvement Act of 1996, the draft JFMIP Financial Management Systems Compliance Review Guide (http://www.financenet.gov/financenet/fed/jfmip/fmscrg.pdf), or other tools. The auditor generally should review this documentation in the internal control phase of the audit to determine the degree to which he or she may rely on it as discussed in section 650. (See section 320.)

.60 If the entity previously had an assessment made of its financial management systems' substantial compliance with these requirements that resulted in lack of substantial compliance, the auditor should read the remediation plan required by FFMIA and note whether the plan appears feasible and likely to remedy the deficiencies.

BUDGET FORMULATION

.61 While assessing the control environment, risk assessment, communication, and monitoring, the auditor should obtain an overall understanding of the budget formulation process. The auditor does this to understand better how misstatements and internal control weaknesses affect the budget

formulation process and, possibly, to consider the budget process as a control. Based on discussions with entity management responsible for the budget formulation process and review of budget documents, the auditor should consider

- the entity's process for developing and summarizing the budget,
- the nature and sufficiency of instructions and training provided to individuals responsible for developing the budget,
- the extent that individuals involved in approving budget requests are also involved in the budget formulation process,
- the general extent to which the budget is based on historical information,
- the reliability of information on which the budget is based,
- the extent to which the budget formulation system is integrated with the budget execution system, and
- the extent of correlation between information developed in the budget formulation process and the allotments and suballotments in the budget execution system.

270 - DETERMINE LIKELIHOOD OF EFFECTIVE INFORMATION SYSTEM CONTROLS

.01 Controls are considered IS controls if their effectiveness depends on computer processing. In the planning phase, the auditor (with the assistance of the IS auditor and using FISCAM or another appropriate methodology) should determine whether IS controls are likely to be effective and should therefore be considered in the internal control phase. The auditor may coordinate work done to meet the requirements of Division A, Title X, Subtitle G (Government Information Security Reform) of the National Defense Authorization Act for Fiscal Year 2001 (P.L. 106-398) with work done as part of the financial statement audit. (See section 295 J for a flowchart of steps in assessing IS controls in a financial statement audit.) The procedures to be performed build on those procedures performed while understanding the entity's operations and assessing the effects of IS on inherent risk and the control environment, risk assessment, communication, and monitoring. AU 319 (SAS 55, as amended by SAS 78 and SAS 94) requires the auditor to sufficiently understand each of the five components of internal control—control environment, risk assessment, information and communications, monitoring, and control activities—to plan the audit. This understanding should include relevant IS aspects.

.02 Computerized financial management systems are used extensively in the federal government. While many of these systems are mainframe based, numerous other technologies also exist. Some of these systems share programs and data files with one another. Others may be networked into major subsystems. In addition to producing financial and accounting information, such systems typically generate other information used in management decision-making.

.03 As discussed in paragraph 260.06, the auditor evaluates and tests the following types of controls in a financial statement audit:

- financial reporting controls,
- compliance controls, and
- certain operations controls (to the extent described in section 275).

.04 For each of the controls to be evaluated and tested, the auditor should distinguish which are IS controls. IS controls–those whose effectiveness

depends on computer processing–can be classified into three types (described in section 295 F):

- general controls,
- application controls, and
- user controls.

Testing of technical IS controls should be performed by an IS auditor as described in section 360. The audit team may assist the IS auditor by testing user controls and application controls involving manual follow-up.

.05 In the planning phase, the auditor and the IS auditor should understand each of the three types of IS controls to the extent necessary to tentatively conclude whether IS controls are likely to be effective. If they are likely to be effective, the auditor should consider specific IS controls in determining whether control objectives are achieved (in the internal control phase).

.06 If IS controls are not likely to be effective, the auditor (with the assistance of the IS auditor) should obtain a sufficient understanding of control risks arising from IS to develop appropriate findings and to plan substantive testing. Also, in the internal control phase, the auditor generally should focus on the effectiveness of manual controls in achieving control objectives. If IS controls are not likely to be effective due to poor general controls and if manual controls do not achieve the control objectives, the auditor should identify and evaluate, but not test, any specific IS controls that are designed to achieve the control objectives (to provide recommendations to improve internal control).

.07 In the planning phase, the auditor and the IS auditor generally limit the understanding of general controls to those at an overall entity level. However, obtaining this understanding generally requires visits to selected installations. General controls related to an installation level and to specific applications will be considered in more detail in the internal control phase. In assessing general controls, the auditor and the IS auditor should consider the results of past internal and external reviews.

.08 The auditor should keep in mind that, as stated in SAS 94, paragraph 66, in some circumstances, such as where a significant amount of information is electronically initiated, recorded, processed, and reported, it may not be

practical or possible to restrict detection risk to an acceptable level by performing only substantive tests for one or more financial statement assertions. In such circumstances, the auditor should test IS controls to obtain evidential matter about the effectiveness of both the design and operation of controls to reduce the assessed level of control risk.

[This page intentionally left blank.]

275 - IDENTIFY RELEVANT OPERATIONS CONTROLS TO EVALUATE AND TEST

.01 The overall intent of the CFO Act is to improve the quality of federal financial management. Reliable financial information and effective internal control are important to the quality of such federal financial management. In a financial statement audit, the auditor draws a conclusion about the effectiveness of certain financial reporting (including safeguarding and budget) and compliance (including budget) controls. For operations controls, the auditor

- may evaluate certain operations controls considered relevant (see paragraphs 275.02-.07),
- should evaluate and test operations controls that are relied on in performing audit procedures (see paragraph 275.08), and
- should understand the components of internal control relating to the existence and completeness (and valuation is required for GAO audits) assertions relevant to the performance measures reported in the MD&A, in order to report on those controls that have not been properly designed and placed in operation, but does not need to test those controls, although he or she may decide to do so (see paragraph 275.09).

RELEVANT OPERATIONS CONTROLS

.02 For the potential operations control needs of the entity or for operations control weaknesses identified through the procedures described in paragraphs 275.04-.07, the auditor should determine whether the evaluation of related controls should (1) be included in the financial audit, (2) become a separate audit, or (3) not be performed but any weaknesses be reported to the IG. In making this determination, the auditor might consider the following factors:

- the significance of the operations control to the entity's operations,
- the time required to identify and test the operations control,
- available resources, and
- congressional interest.

.03 Audit team management should agree on the operations controls that are to be evaluated and tested as part of the financial audit. Such operations

controls should be documented in the workpapers. For example, audit management may require that before evaluating and testing a specific operations control, the audit team submit relevant information to audit management on a standard form developed by the audit team.

.04 In the planning phase and throughout the audit, the auditor generally should identify significant areas where the entity would be expected to have operations controls. The auditor may become aware of these areas, as well as potential weaknesses in operations controls, through

- understanding the entity's operations.
- planning the audit procedures,
- understanding audit risks and weaknesses in financial reporting and compliance controls,
- understanding the cause of misstatements noted, or
- observations made during on-site fieldwork.

.05 In obtaining an understanding of the entity's operations, the auditor should identify those areas that are critical to such operations. For each of these areas, the entity should have effective operations controls. Also, in planning the audit, the auditor may identify operations controls that could be evaluated in conjunction with planned audit and other procedures. For example, the auditor may evaluate whether management considered appropriate order quantities for each inventory purchase selected in a test of inventory purchases.

.06 The auditor identifies specific risks and weaknesses in planning and performing the audit and in determining the causes of misstatements requiring audit adjustments. The auditor should consider the implications of those risks and weaknesses on the entity's operations controls. For example, misstatements in inventory records may indicate weaknesses in operations controls whose effectiveness depends on accurate inventory records. This would include the operations controls for maintaining proper inventory levels.

.07 The auditor should be alert to any opportunities to recommend improvements to operations controls. Such opportunities could come to light while visiting the entity's various locations and performing the financial audit.

OPERATIONS CONTROLS RELIED ON IN THE AUDIT

.08 If any contemplated audit procedure relies on operations controls, the auditor should identify and test such controls. For example, assume that an auditor is using substantive analytical procedures, based on entity-generated "per unit" statistics, to test the reasonableness of certain operating costs. The auditor plans to compare such "per unit" statistics with published costs incurred by similar operations. The auditor will need to identify and test the entity's operations controls over the production of these internal statistics.

OPERATIONS CONTROLS OVER REPORTED PERFORMANCE MEASURES

.09 OMB audit guidance requires the auditor to understand the design of internal controls over the existence and completeness (see definition in paragraph 235.02) assertions (and GAO has added valuation as a requirement for its audits) related to the performance measures the entity reports on in the MD&A and whether they have been placed in operation. However, OMB does not require the auditor to test the controls (determine operating effectiveness), although he or she may decide to do so. The procedures the auditor performs to gain the understanding do not need to be extensive but may consist of discussions, observations, and walkthroughs (see AU 319.41-.43).

[This page intentionally left blank.]

280 - PLAN OTHER AUDIT PROCEDURES

.01 The auditor should consider the following areas during the planning phase, even though many related audit procedures will be applied during the other phases.

INQUIRIES OF LEGAL COUNSEL

.02 As discussed in AU 337 and section 550, the auditor should make inquiries of the entity's counsel and perform other audit procedures regarding litigation, claims, and assessments. Because of the amount of the time needed by management and the legal counsel to gather and report the necessary information (including the potential need for management to inquire of Department of Justice legal counsel on a case-specific basis), the auditor should plan the following procedures (which are described in more detail in AU 337) for an appropriate time in the audit:

- making inquiries of management regarding their policies and procedures used for identifying, evaluating, and accounting for litigation, claims, and assessment;
- obtaining a description and evaluation of all such matters existing as of the balance sheet date and through the date of management's response (which should be near the end of fieldwork);
- obtaining evidence regarding legal counsel used by the entity and matters handled; and
- sending letters of audit inquiry to legal counsel (the auditor may limit the inquiry to matters that are considered individually or collectively material to the financial statements, provided the entity and the auditor have reached an understanding and agreement on the materiality level).

MANAGEMENT REPRESENTATIONS

.03 As discussed in section 550, the auditor is required to obtain a representation letter from management on specific matters prior to completion of the audit. Particularly during first year audits and when standards change, the auditor may want to discuss these required representations with management early in the audit to identify and resolve any difficulties related to obtaining these representations. Note that for federal government auditors, these representations include (1) the effectiveness of internal control, (2) compliance with laws and regulations, and, (3) for CFO Act agencies, financial management systems' substantial compliance with FFMIA requirements. Additional guidance on management representations is provided in AU 333, AU 801, AT 101, AT 201, AT

501, AT 601, and section 1001 (Part II). Also, a summary of uncorrected misstatements aggregated by the auditor is to be included or attached to the letter, which should state management's belief that the effects of the misstatements are immaterial to the financial statements taken as a whole, both individually and in the aggregate. (See section 595 D for an example summary of uncorrected misstatements.)

RELATED PARTY TRANSACTIONS

.04 AU 334 and sections 550 and 902 provide guidance on audit procedures that should be performed to identify related parties and related party transactions as well as examining these transactions for appropriate disclosure in the financial statements. During the planning phase, the auditor should perform procedures to identify and document related parties and the nature of related party transactions that might need to be disclosed in the financial statements and related notes. Such information should be distributed to all members of the audit team for use in summarizing and testing related party transactions and identifying any additional related parties.

SENSITIVE PAYMENTS

.05 In the planning phase, the auditor should consider the audit procedures that will be applied to sensitive payments. Sensitive payments encompass a wide range of functions, including executive compensation, travel, official entertainment funds, unvouchered expenditures, consulting services, speaking honoraria and gifts, and executive perquisites. See GAO's *Guide for Evaluating and Testing Controls Over Sensitive Payments*, GAO/AFMD-8.1.2, Washington, D.C.: May 1993.

REACHING AN UNDERSTANDING WITH OFFICIALS OF THE ENTITY AND REQUESTERS

.06 During planning, the auditor should reach an understanding with officials of the entity, including management and individuals contracting for or requesting the audit, about the work to be performed, as required by AU 310 and GAGAS (chapter 4). If the audit is done based on the request of a committee or member of Congress, the auditor should communicate with that committee or member as well as management. If the audit is required by law or is self-initiated, the auditor should communicate with the committee members or staff who have oversight of the auditee as well as management.

.07 The auditor should communicate with officials of the entity and the committee or member in writing (preferred) or orally and document the understanding reached. "Commitment" letters may be used to communicate with Congress about the

auditor's planned work. In drafting commitment letters, the auditor should consider the matters required to be communicated by the auditing standards. If the audit organization has a general ongoing working relationship with Congress and prior audit reports, there may already be an understanding with the applicable committee or other requester.

.08 Because of an ongoing working relationship with either a requester or management, the auditor may affirm the contents of the prior audit report, since the types of information included in the understanding are generally included in the objectives, scope, and methodology section of the audit report.

.09 Examples of the matters that are generally included in the understanding are the objectives and limitations of the audit and management's and the auditor's responsibilities. These are described in AU 310. GAGAS also require the understanding to relate to the auditor's responsibility for testing and reporting on compliance and internal control.

OTHER AUDIT REQUIREMENTS

.10 Under GAGAS, chapter 4, the auditor should consider the results of previous audits and attestation engagements and follow up on known significant findings and recommendations that relate directly to the objectives of the current audit. Generally, a financial audit should cover areas that had findings and recommendations in previous audits. However, the auditor should consider whether any findings and recommendations from the prior year financial audit need follow-up that would not otherwise be covered (for example, findings at locations that would not otherwise be revisited).

.11 During planning, the auditor also should consider the additional requirements in OMB audit guidance for legal letters, management representation letters, and certain agreed-upon procedures. OMB audit guidance has specific dates by which interim and updated legal letters for CFO Act agencies and covered executive agencies subject to the Accountability of Tax Dollars Act of 2002[1] are to be requested and received, specific formats for summarizing the information in the letters, and a list of specific officials to whom copies of the letters and summaries should be forwarded. The guidance also has an example of a management representation letter. In addition, the guidance requires that certain agreed-upon procedures be applied to agency payroll offices and requires that reports be submitted to OPM by a specific date.

[1] OMB issued guidance implementing the act by applying its guidance for CFO Act agencies to covered executive agencies.

[This page intentionally left blank.]

285 - PLAN LOCATIONS TO VISIT

.01 Most federal entities conduct operations, perform accounting functions, and/or retain records at multiple locations. During planning, the auditor needs to consider the effect of these multiple locations on the audit approach. The auditor should develop an understanding of the respective locations, including significant accounts and accounting systems and cycles/applications. This understanding may be obtained centrally or in combination with visits to field offices, as appropriate. When planning locations to visit, the auditor should consider whether certain locations warrant more extensive testing than others, based on the following factors:

- **Materiality or significance of locations to the overall entity:** More material locations, particularly those individually exceeding design materiality, and significant cycles/accounting applications may require more extensive testing.

- **The results of the preliminary analytical procedures applied during planning:** Unusual results require follow-up, possibly including on-site testing at specific locations causing such results.

- **The results and the extent of audit procedures applied in prior years by the auditor or others, including the time since significant procedures were performed:** Problems noted in prior audits could indicate areas of concern for the current audit, and the effectiveness of prior evidence ordinarily diminishes with the passage of time.

- **The auditor's assessment of inherent risk, including the nature of operations, sensitivity to economic conditions, and key management turnover:** Locations at which inherent risk is high generally warrant more extensive testing than those where inherent risk is low.

- **The auditor's preliminary assessment of control risk, including the control environment, risk assessment, communications, and monitoring:** Locations at which control risk (particularly concerning the control environment, risk assessment, communication, and monitoring) is high warrant more extensive testing than those where control risk is low.

- **The auditor's consideration of the risk of material misstatement due to fraud:** Locations at which the auditor has considered there may be a greater risk of material misstatement due to fraud warrant more extensive testing than those where he or she has considered a lower risk of material misstatement due to fraud is present.

- **The extent to which accounting records are centralized:** A high degree of centralization may enable the auditor to conduct the majority of work at the central location, with only limited work at other locations.

- **The extent of uniformity of control systems (including computer controls) throughout the entity:** The number of locations visited is a function of the uniformity of significant control systems. For example, if there are two major procurement control systems, the auditor generally should test each system to a sufficient extent. Where locations develop or modify systems, more locations may require visits than for those entities using centrally developed systems that cannot be changed locally.

- **The extent of work performed by other auditors:** Work done by other auditors may be used to reduce or eliminate tests at selected locations or to assist in tests of locations not selected. (See section 650.)

- **Special reporting or entity requirements:** The auditor should select sufficient locations to meet special needs, such as separate-location reports.

.02 The auditor should plan the general nature of audit procedures to be performed at each location. The extent of testing may vary between locations, depending on test materiality, control risk, and other factors. Using common audit programs, workpaper formats, and indexes for the various locations visited makes it easier to plan, review the workpapers, and combine the results of all locations or funds to improve effectiveness and efficiency.

.03 The auditor should obtain an understanding of the procedures for combining the locations' financial information to prepare the entity's financial statements. The auditor should understand and test these procedures during the audit, including any necessary adjustments and eliminations.

.04 One approach to stratifying the locations and selecting samples for multiple-location audits is provided in section 295 C. This method assumes that increased testing is not required at any location because of the factors in paragraph 285.01. Other methods of selecting locations for on-site testing may be used with the approval of the Reviewer. For example, selecting fewer locations but more items to test at each of those locations may be appropriate in some instances. Although other methods generally will require more overall audit testing than the method described in section 295 C, the costs of performing additional work at fewer locations may be lower.

[This page intentionally left blank.]

290 - DOCUMENTATION

.01 The auditor should document relevant information obtained during the planning phase in the documents described in paragraphs 290.03-.06. Also, as described in paragraph 290.07, the auditor should document the understanding reached with requesters and management. Information that is likely to be useful in future audits may be documented in a permanent file.

.02 As the audit work is performed, the auditors may become aware of possible reportable conditions or other matters that should be communicated to the auditee. A structured method to document these matters will aid in communicating them to the audit team, management for review, and the agency soon after their discovery. The auditor generally should document the nature of the reportable condition and the criteria, cause, potential effect, and suggestions for improvement (as applicable) throughout the audit and discuss them with management when identified, rather than waiting until the exit conference.

.03 In the **entity profile** or an equivalent document, the auditor should document the information gathered to gain an understanding of the entity (section 220). This profile should briefly document such elements as the entity's origin and history, size and location, organization, mission, results of prior and current audits, and accounting and auditing considerations. The auditor generally should limit the information in the entity profile to that which is relevant to planning the audit. This information may include documents prepared by the entity, such as historical information or the mission of the entity. If this and other documents were prepared in prior years, they need only be updated for changes each year.

.04 The **General Risk Analysis** or an equivalent document contains the overall audit plan, including the strategy for conducting the audit, and also should include information on the following areas:

a. **Preliminary analytical procedures and the results of those procedures (section 225):** The auditor should document the following information:

- data used and sources of financial data used for current-year amounts and for developing expected amounts, including

- - the amounts of the financial items,
  - the dates or periods covered by the data,
  - whether the data are audited or unaudited,
  - the person from whom the data were obtained (if applicable), and
  - the source of the information (for example, the general ledger trial balance, prior-year audit workpapers, or prior-year financial statements);

- parameters for identifying significant fluctuations;

- explanations for fluctuations identified and sources of these explanations, including the name and title of the person(s) from whom the explanations were obtained; and

- the auditor's conclusion and consideration of the impact of the results of preliminary analytical procedures on the audit.

b. **Planning, design, and test materiality, including the basis for their determination (section 230).**

c. **Methodology used in assessing computer-related controls (section 240):** If the auditor uses a methodology other than the FISCAM, he or she should document the basis for believing that the methodology is appropriate.

d. **Significant provisions of laws and regulations (section 245).**

e. **Relevant budget restrictions (section 250).**

f. **Level of audit assurance (section 260):** The auditor should document the overall level of audit assurance and the justification for the level used. If the level of audit assurance chosen is 95 percent, the auditor may reference the FAM.

g. **Assessment of inherent risk and the overall effectiveness of the control environment, risk assessment, communication, and monitoring, including whether they preclude the effectiveness of specific control activities (section 260):** The auditor identifies and documents any inherent risks or control risks arising from the control environment, risk assessment, communication, and monitoring and

associates them with significant financial statement line items and assertions. For each risk identified, the auditor documents the (1) nature and extent of the risk, (2) condition(s) that gave rise to that risk, and (3) specific cycles, accounts, line items, and related assertions affected (if not pervasive). The auditor also documents conclusions on the overall effectiveness of the control environment, risk assessment, communication, and monitoring. In addition, the auditor generally should document the entity's basis for its determination of substantial compliance of its systems with FFMIA requirements.

h. **Fraud risks (section 260)**. The auditor should document (also see paragraph 290.07):

- specific fraud risks (categorized by type of misstatement and by incentive/pressure, opportunity, and attitude/rationalization) that were identified and the assessment of those risks;
- if the auditor did not consider improper revenue recognition to represent a fraud risk, the reasons supporting that conclusion;
- consideration of the risk of management override of controls; and
- the auditor's response to the assessed fraud risks. (Also see section 590.)

i. **Effects of IS (section 270):** The auditor should document

- a basic understanding of the IS aspects of the financial management system, including the significance of IS to the entity (section 220);
- the inherent risks arising from IS (paragraph 260.17);
- the impact of IS on the control environment, risk assessment, communication, and monitoring (paragraphs 260.41-.42); and
- tentative conclusions on the likelihood that IS controls are operating effectively (section 270).

When the auditor prepares documentation of the above information, the IS auditor generally should review and agree with the content. Tentative conclusions on the likelihood that IS controls are operating effectively should also be reviewed and concurred to by the Audit Director and Assistant Director as part of their reviews of the General Risk Analysis or equivalent. If IS controls are not likely to be effective, the auditor should document supporting evidence and generally should report such findings as discussed in section 580.

j. **Operations controls to be tested, if any (section 275).**

k. **Other planned audit procedures (section 280).**

l. **Locations to be visited (section 285):** This information includes

- the locations selected,
- the basis for selections,
- the general nature of procedures planned for each location,
- the determination of the number of items for testing,
- the allocation of those items among the selected locations, and
- other procedures applied.

m. **Staffing requirements.**

n. **Audit timing, including milestones.**

o. **Assistance from entity personnel.**

.05 The **Cycle Matrix** or equivalent links each of the entity's accounts (in the chart of accounts) to a cycle, an accounting application, and a financial statement line item or RSSI (paragraph 240.06). This information may instead be incorporated into the Account Risk Analysis or equivalent.

.06 The **Account Risk Analysis** or equivalent contains the audit plan for each significant line item and account and should identify significant line items, accounts, assertions, and cycles/accounting applications (sections 235 and 240, respectively). The auditor also summarizes and documents the specific risks, other than pervasive risks, as well as the inherent, fraud, and control risk factors, for use in determining the nature, timing, and extent of the audit procedures. The auditor may also include insignificant accounts in each line item ARA or equivalent, indicating their insignificance and the consequent lack of audit procedures applied to them. In such instances, the cycle matrix or equivalent need not be prepared.

.07 The auditor also should document (section 260):

- the brainstorming meeting(s) about potential fraud risks, including how and when the discussion(s) occurred, the audit team members who participated, and the general matters discussed;
- the procedures performed to obtain information about, identify, and assess fraud risks; and
- any other significant procedures performed or other significant matters related to the auditor's consideration of fraud (and any significant abuse).

.08 The auditor should document the understanding reached with officials of the entity and requesters about the work to be performed, as described in section 280.

.09 The auditor also should consider the needs of, and consult in a timely manner with, other auditors who plan to use the work being performed, especially in areas where the auditor makes decisions requiring significant auditor judgment. Where the auditor deviates from a policy or procedure expressed by use of the term “must” or “should” in the FAM, he or she should provide an opportunity for the other auditors to review the documentation of the reasons explaining these deviation decisions.

[This page intentionally left blank.]

295 A - POTENTIAL INHERENT RISK CONDITIONS

.01 The specific conditions listed below may indicate the presence of inherent and/or fraud risks. This section is designed to aid the auditor in considering each of the inherent risk factors described in paragraph 260.16 and the fraud risk factors described in paragraphs 260.24-.25 relating to industry conditions, operating conditions and financial stability, and susceptibility of assets to misappropriation, but is not intended to be all inclusive. The auditor should consider any other factors and conditions considered relevant.

.02 **NATURE OF THE ENTITY'S PROGRAMS**

- Programs are significantly affected by new/changing governmental regulations, economic factors, and/or environmental factors.
- Contentious or difficult accounting issues are associated with the administration of a significant program(s).
- Major uncertainties or contingencies, including long-term commitments, relate to a particular program(s).
- New (in existence less than 2 years) or changing (undergoing substantial modification or reorganization) programs lack written policies or procedures, lack adequate resources, have inexperienced managers, lack adequate systems to measure performance, and generally have considerable confusion associated with them.
- Programs that are being phased out (being eliminated within 1 or 2 years), lack adequate resources, lack personnel motivation and interest, or involve closeout activities for which controls have not been developed.
- Significant programs have a history of improper administration, affecting operating activities.
- Significant programs have a history of inadequate financial management systems causing management to resort to extensive, costly, time-consuming, ad hoc efforts to prepare financial statements by the required deadline.

- Significant programs have minimal IG or internal audit coverage.

- Management faces significant pressure to obtain additional funding necessary to stay viable and maintain levels of service considering the financial or budgetary position of a program, including the need for funds to finance major research and development or capital expenditures.

- Management faces significant pressure to "use or lose" appropriated funds in order to sustain future funding levels.

- Partisan politics between competing political parties or factions or constituent groups create conflict and a lack of stability within the entity or programs.

- Unusually rapid growth occurs in a program.

- Economic conditions are deteriorating among the group served by the entity.

.03 HISTORY OF SIGNIFICANT AUDIT ADJUSTMENTS

- The underlying cause of significant audit adjustments continues to exist.

.04 NATURE OF MATERIAL TRANSACTIONS AND ACCOUNTS

- New types of transactions exist.

- Significant transactions or accounts have minimal IG or internal audit coverage.

- Significant related and/or third party transactions exist.

- Classes of transactions or accounts are

  - difficult to audit;
  - subject to significant management judgments (such as estimates);
  - susceptible to manipulation, loss, or misappropriation;
  - susceptible to inappropriate application of an accounting policy; and
  - susceptible to problems with realization or valuation.

- Accounts have complex underlying calculations or accounting principles.
- Accounts in which the underlying activities, transactions, or events are operating under severe time constraints.
- Significant interagency transactions or revenue sources create incentives to shift costs or otherwise manipulate accounting transactions.
- Accounts in which activities, transactions, or events involve the handling of unusually large cash receipts, cash payments, or wire transfers.
- Inventory or equipment have characteristics such as small size, high value, high demand, marketability, or lack of ownership identification that make them easily converted to cash (for example, pharmaceutical inventory or military equipment with high street values).
- Assets are easily converted to cash, such as food stamps, benefits vouchers, commodities, supplies, or materials.
- Assets are susceptible to personal, non-program/non-government use such as cars, computers, telephones.
- Many payments are sent to post office boxes.
- Large amounts of payments are sent to outside recipients, as in the cases of grants, medical care reimbursements, or other federal financial assistance.

[This page intentionally left blank.]

295 B - POTENTIAL CONTROL ENVIRONMENT, RISK ASSESSMENT, COMMUNICATION, AND MONITORING WEAKNESSES

.01 The specific conditions listed below may indicate the presence of control environment, risk assessment, communication, and monitoring weaknesses and fraud risk. This section is designed to aid the auditor in considering each of the control environment, risk assessment, communication, and monitoring factors described in paragraphs 260.32-.40 but is not intended to be all inclusive. The auditor should consider any other factors and conditions considered relevant. (If the auditor is doing a more detailed assessment of internal control than is usual in a financial audit, he or she may refer to GAO's exposure draft of *Internal Control Management and Evaluation Tool* for additional and more detailed examples of internal control factors.)

CONTROL ENVIRONMENT

.02 **Integrity and Ethical Values**

- An appropriate "tone at the top" has not been established and communicated throughout the entity, including explicit moral guidance about what is right and wrong.
- No (or inadequate) formal code of conduct or other policies regarding acceptable practices, conflicts of interest, or expected standards of ethical and moral behavior exists, or employees are unaware of it.
- Employees do not understand what behavior is acceptable or unacceptable, or what to do if they encounter improper behavior.
- Bad news is covered up by management rather than making full disclosure as quickly as possible.
- Management does not quickly address signs that problems exist.
- Employees feel peer pressure to cut corners.

- High decentralization leaves top management unaware of actions taken at lower organizational levels and thereby reduces the chances of getting caught.
- Everyday dealings with employees, auditors, the public, oversight groups, etc., are not generally based on honesty and fairness (for example, overpayments received or supplier underpayments are ignored, or efforts are made to find a way to reject legitimate benefits claims).
- Penalties for improper behavior are insignificant or unpublicized and thus lose their value as deterrents.
- Management has displayed a loose attitude towards internal control, for example, by not providing guidance on when intervention is allowed or not investigating and documenting deviations.
- Pressure is felt to meet performance targets or deadlines that are unrealistic.
- Management is under undue pressure from the administration to attain an unqualified opinion on the financial statements, despite significant internal control weaknesses.
- Management displays lack of candor in dealing with oversight committee staff, recipients of the entity's services, or auditors regarding decisions that could have an impact on the entity.

.03 **Commitment to Competence**

- Jobs have not been analyzed to determine the knowledge and skills needed.
- Employees do not seem to have the knowledge and skills they should have to do their jobs, based on the level of judgment necessary.
- Supervision of employees does not compensate for lack of knowledge and skills in their specific jobs.

.04 Management's Philosophy and Operating Style

- Management lacks concern about internal control and the environment in which specific controls function.
- Management demonstrates an aggressive approach to risk-taking.
- Management demonstrates an aggressive approach to accounting policies.
- Management has a history of completing significant or unusual transactions near the year's end, including transactions with related parties.
- Management makes numerous adjusting journal entries, especially at yearend.
- Management is reluctant to (1) consult auditors/consultants on accounting issues, (2) adjust the financial statements for misstatements, or (3) make appropriate disclosures.
- Management displays a significant disregard for regulatory, legal, or oversight requirements or for IG, GAO, or Congressional authorities.
- Top-level management lacks the financial experience/background necessary for the positions held.
- Management is slow to respond to crisis situations in both operating and financial areas.
- Management uses unreliable and inaccurate information to make business decisions.
- Unexpected reorganization or replacement of management staff or consultants occurs frequently.
- Management and personnel in key areas (such as accounting, IS, IG, and internal auditing) have a high turnover.

- Individual members of top management are unusually closely identified with specific major projects.

- Overly optimistic information on performance of programs and activities is disclosed.

- Financial estimates consistently prove to be significantly overstated or understated.

- Obtaining adequate audit evidence is difficult due to a lack of documentation and evasive or unreasonable responses to inquiries.

- Financial arrangements/transactions are unduly complex.

- Lack of interaction of adequate frequency between senior management and operating management, particularly with geographically removed locations.

- Management attitude toward IS and accounting functions is that these are necessary "bean counting" functions rather than a vehicle for exercising control over the entity's activities.

- Management is motivated to engage in fraudulent financial reporting resulting from substantial political pressure creating an undue concern about reporting positive financial accomplishments.

- Management is dominated, either entity-wide or at a specific component, by a single person or small group without compensating controls such as effective oversight by the IG, GAO, Congressional committees, or other oversight body.

- One or more individuals with no apparent executive position(s) with the entity appear to exercise substantial influence over its affairs or over individual departments or programs (for example, a major political donor or fundraiser).

- Management has significant grantee, cooperative agreement, or contractor relationships for which there appears to be no clear programmatic or governmental justification.

- Management appears more concerned with an unqualified opinion on the financial statements rather than with fixing significant weaknesses in its systems.

- Management has difficulty meeting reporting deadlines.

.05 **Organizational Structure**

- The organizational structure is inappropriate for the entity's size and complexity. General types of organizational structures include

  - federal centralized (managed and controlled on a day-to-day basis by a centralized federal entity system),

  - federal decentralized (managed and controlled on a day-to-day basis by federal entity field offices or staffs),

  - participant administered (managed and controlled on a day-to-day basis by a nonfederal organization), and

  - other (managed and controlled on a day-to-day basis by some combination of the above or by other means).

- The structure inhibits segregation of duties for initiating transactions, recording transactions, and maintaining custody over assets.

- It is difficult to determine the organization or individual(s) that control(s) the entity, parts of the entity, or particular programs.

- Recent changes in the management structure disrupt the organization.

- Operational responsibilities do not coincide with the divisional structure.

- Delegation of responsibility and authority is inappropriate.

- A lack of definition and understanding of delegated authority and responsibility exists at all levels of the organization.

- Inexperienced and/or incompetent accounting personnel are responsible for transaction processing.
- The number of supervisors is inadequate or supervisors are inaccessible.
- Key financial staff have excessive work loads.
- Policies and procedures are established at inappropriate levels.
- A high degree of manual activity is required in capturing, processing, and summarizing data.
- Activities are dominated and controlled by a single person or a small group.
- The potential exists for entity officials to obtain financial or other benefits on the basis of decisions made or actions taken in an official capacity.

.06 **Assignment of Authority and Responsibility**

- The entity's policies are inadequate regarding the assignment of responsibility and the delegation of authority for such matters as organizational goals and objectives; operating functions; and regulatory requirements, including responsibility for information systems and authorizations for changes.
- Appropriate control-related standards and procedures are lacking.
- The number of people, particularly in IS and accounting, with requisite skill levels relative to the size and complexity of the operations is inadequate.
- Delegated authority is inappropriate in relation to the assigned responsibilities.
- Appropriate system of authorization and approval of transactions (for example, in purchasing, grants, and federal financial assistance) is lacking.

- Policies are inadequate regarding physical safeguards over cash, investments, inventory, and fixed assets.

.07 **Human Resource Policies and Practices**

- Human resource policies for hiring and retaining capable people are inadequate.
- Standards and procedures for hiring, promoting, transferring, retiring, and terminating personnel are insufficient.
- Training programs do not adequately offer employees the opportunity to improve their performance or encourage their advancement.
- Written job descriptions and reference manuals are inadequate or inadequately maintained.
- Communication of human resource policies and procedures at field locations is inadequate.
- Policies on employee supervision are inappropriate or obsolete.
- Inappropriate remedial actions are taken in response to departures from approved policies and procedures.
- Employee promotion criteria and performance evaluations are inadequate in relation to the code of conduct.
- Job applicant screening procedures for employees with access to assets susceptible to misappropriation are lacking.
- Training is inadequate regarding controls over payments to others for grants, federal financial assistance, etc.
- Mandatory vacations are not required for employees performing key control functions.

.08 Management's Control Methods Over Budget Formulation and Execution

- Little or no guidance material and instructions are available to provide direction to those preparing the budget information.
- The budget review, approval, and revision process is not defined or understood.
- Management demonstrates little concern for reliable budget information.
- Management participation in directing and reviewing the budget process is inadequate.
- Management is not involved in determining when, how much, and for what purpose obligations and outlays can be made.
- The planning and reporting systems that set forth management's plans and the results of actual performance are inadequate.
- Inadequate methods are used to identify the status of actual performance and exceptions from planned performance and communicate them to the appropriate levels of management.
- Noncompliance with Antideficiency Act, purpose, time, or other budget-related restrictions has been previously reported.

.09 Management's Control Methods Over Compliance with Laws and Regulations

- Management is unaware of the applicable laws and regulations and potential problems.
- A mechanism to inform management of the existence of illegal acts does not exist.
- Management neglects to react to identified instances of noncompliance with laws and regulations.

- Management is reluctant to discuss its approach toward compliance and the reasonableness of that approach.

- Recurring public complaints have been received through "hotline" allegations.

- Repeated instances of noncompliance or control weaknesses are disclosed in FMFIA reports; congressional reports; consultants' reports; and prior audits/evaluations by GAO, the IG, internal audit, or others.

- Management is reluctant to provide evidential matter necessary to evaluate whether noncompliance with laws and regulations has occurred.

- Management is not responsive to changes in legislative or regulatory bodies' requirements.

- Policies and procedures for complying with laws and regulations are weak.

- Policies on such matters as acceptable business practices, conflicts of interest, and codes of conduct are weak.

- Management does not have an effective legal counsel.

.10 Oversight Groups (Including Congressional Committees)

- Oversight groups demonstrate little concern toward controls and the speed with which internal and external auditors' recommendations are addressed.

- Oversight groups have little involvement in and scrutiny of activities.

- Little interaction occurs between oversight groups and the IG and internal and external auditors.

- Oversight groups demonstrate little concern for compliance with applicable laws, regulations, and contractual requirements.

RISK ASSESSMENT

.11 Setting Objectives

- Management has not established or communicated its overall objectives to employees or oversight committees.
- No strategic planning has been done, or the strategic plan does not support the objectives.
- The strategic plan does not address high-level resource allocations and priorities.
- The strategic plan, budgets, and/or objectives are inconsistent.
- Management has not established activity-level objectives for all significant activities, or the objectives are inconsistent with each other or with the overall objectives.
- Objectives do not include measurement criteria.

.12 Analyzing Risks

- Management has not adequately identified risks to achieving the entity's objectives arising from external sources, including economic conditions, the President, the Congress, OMB, and the media.
- Management has not adequately identified risks arising from internal sources, such as human resources (ability to retain key people) or IS (adequacy of back-up systems in the event of systems failure).
- Once risks are identified, management has not adequately analyzed the risks, including estimating the significance of risks, assessing the likelihood of their occurring, and determining needed actions.

.13 **Managing Change**

- The mechanisms for identifying and communicating events, activities, and conditions that affect operations or financial reporting objectives are insufficient.

- Accounting and/or information systems are not modified in response to changing conditions.

- No consideration is given to designing new or alternative controls in response to changing conditions.

- Management is unresponsive to changing conditions.

COMMUNICATION

.14 **Internal Communication**

- The system for communicating policies and procedures is ineffective.

- Formal or informal job descriptions do not adequately delineate specific duties, responsibilities, reporting relationships, and constraints.

- Channels of communication for personnel reporting suspected improprieties are inappropriate.

- Management fails to display and communicate an appropriate attitude regarding internal control.

- Management is not effective in communicating and supporting the entity's accountability for public resources and ethics, especially regarding matters such as acceptable business practices, conflicts of interest, and codes of conduct.

- Management is not receptive to employee suggestions of ways to enhance productivity and quality or other similar improvements.

- Communication across the organization (for example, between procurement and program activities) is inadequate to enable people to discharge their responsibilities effectively.

.15 **External Communication**

- Channels of communication with suppliers, contractors, recipients of program services, and other external parties are not open and effective for communicating information on changing needs.

- Outside parties have not been made aware of the entity's ethical standards.

- Management does not appropriately follow up on information received in communications from program service recipients, vendors, regulators, or other external parties.

MONITORING

.16 **Ongoing Monitoring**

- Management is not sufficiently involved in reviewing the entity's performance.

- Management control methods are inadequate to investigate unusual or exceptional situations and to take appropriate and timely corrective action.

- Management lacks concern for and does not effectively establish and monitor policies for developing and modifying accounting systems and control activities.

- Management's follow-up action is untimely or inappropriate in response to communications from external parties, including complaints, notification of errors in transactions with parties, and notification of inappropriate employee behavior.

- Management does not periodically compare amounts recorded by the accounting system with physical assets.

- Management allows large numbers of duplicate payments.
- Management does not respond to internal and external auditors' recommendations to strengthen internal control.
- Management has strained relationships with the IG and/or its current or predecessor external auditors.
- Management does not encourage and consider employee suggestions.
- Personnel do not periodically acknowledge compliance with the code of conduct or sign off to evidence performance of critical control functions.
- Management does not adequately monitor significant activities that have been outsourced to contractors or information systems components maintained by contractors.

.17 FMFIA or Similar Separate Evaluations

- Management displays a disregard for fully complying with the FMFIA process, reporting, results, and follow-up.
- Management displays a disregard for fully complying with or a combative attitude towards the FFMIA process, reporting, results, and follow-up.
- FMFIA or similar reviews are not conducted by personnel with requisite skills or using a logical and appropriate methodology.
- Auditors note weaknesses that were not included in FMFIA and FFMIA reports.

.18 Reporting Deficiencies

- The entity does not have a mechanism for capturing and reporting identified internal control deficiencies from both internal and external sources resulting from ongoing monitoring or separate evaluations.

- Deficiencies are not reported to the person with direct responsibility and to a person at least one level higher or to more senior management for specified types of deficiencies.

- Corrective actions on deficiencies do not take place on a timely basis.

- Underlying causes of problems are not investigated.

- Follow-up to ensure that the necessary corrective action has taken place is not done.

.19 **The Effectiveness of Other Auditors**

- The audit staff are responsible for making operating decisions or for controlling other original accounting work subject to audit.

- Audit management personnel are inexperienced for the tasks assigned.

- Training activities are minimal, including little or no participation in formal courses and seminars and inadequate on-the-job training.

- Resources to effectively conduct audits and investigations are inadequate.

- Audits are not focused on areas of highest exposure to the entity.

- Standards against which the auditor's work is measured are minimal or nonexistent.

- Performance reviews are nonexistent or irregular.

- The audit planning process is nonexistent or inadequate, including little or no concentration on significant matters and little or no consideration of the results of prior audits and current developments.

- Supervision and review procedures are nonexistent or inadequate, including little involvement in the planning process, in monitoring progress, and in reviewing conclusions and reports.

- Workpaper documentation (audit programs, evidence of work performed, and support for audit findings) is incomplete.

- An inadequate mechanism is used to keep the entity head and the Congress informed about problems, deficiencies, and the progress of corrective action.

- Audit coverage over payments made by others (such as states) for grants, federal financial assistance, etc. is inadequate.

- The audit has an inadequate review of computer general and application controls.

- The auditor does not use appropriate tools, such as audit software and sampling.

- The audit department does not have a peer review every 3 years.

- The audit department does not have an annual internal inspection.

[This page intentionally left blank.]

295 C - AN APPROACH FOR MULTIPLE-LOCATION AUDITS

.01 This section provides one approach for stratifying the locations and selecting the samples for multiple-location audits. This method assumes that the auditor first identifies locations to be tested each year because of specific inherent or control risks. Other methods of selecting locations for on-site testing may be used with the approval of the Reviewer.

STRATIFYING THE LOCATIONS

.02 Unless a dollar-unit sampling method is used, which automatically stratifies the population, the auditor stratifies the locations by separating them into an appropriate number of relatively homogeneous groups or strata. Stratification can improve the efficiency of the sample result (reduce the uncertainty of the estimate) by grouping items together that are expected to behave similarly with respect to the audit measure. Stratification can also be used to ensure that items of special interest receive adequate coverage in the sample. The stratification should be based on relative size and/or qualitative factors, such as inherent or control risk. If exact information is not available, estimates may be used. Criteria for stratifying may include one or more of the following relative factors:

- the amount of assets;
- the amounts of revenue and expenses incurred or processed at the location;
- the number of personnel, where payroll costs are significant;
- the amount of appropriations;
- a concentration of specific items (such as a stratum consisting of significant inventory storage locations, of which those selected will undergo only inventory procedures);
- the nature and extent of inherent and control risk, including fraud risk and sensitive matters or the turnover of key management; and

- special reporting requirements, such as separate reports, special disclosures, or supplementary schedules.

.03 For example, the auditor may stratify locations, based on the amount of total assets, into the following strata: (1) individually material locations (top stratum), (2) relatively significant locations (intermediate stratum), and (3) relatively insignificant locations (bottom stratum). If an entity has 100 locations and if the total amount of assets is determined to be the relevant criterion for stratifying locations, the first three columns of table 295 C.1 may represent an acceptable stratification.

.04 SELECTING LOCATIONS

The auditor selects locations for on-site testing using one of the following methods for each stratum: (These methods are described in more detail in section 480.)

- Dollar-unit sampling (DUS) or classical variables sampling using a multistage approach may be used as described in section 480.
- Another representative sampling method may be used when appropriate. The auditor should consult with the Statistician if classical variables sampling or another representative sampling method is used.
- Nonrepresentative selection (nonsampling) is used when the auditor determines that it is effective to select locations on a nonrepresentative basis and to apply substantive analytical procedures and/or other substantive tests to locations that are not tested on-site.

.05 Table 295 C.1 illustrates a possible DUS sample for each stratum, using design materiality of $3 million and 95-percent assurance. For a DUS sample, the sampling interval would be $1 million, and the preliminary estimate of the sample size would be 100 ($100 million divided by $1 million). Section 400 provides additional information on calculating the amounts in the table and the various selection methods.

TABLE 295 C.1: EXAMPLE OF DUS SAMPLING

Stratum	Number of locations	Assets	Preliminary estimate of sample size[a]	Actual number of locations tested[b]
Top	5	$ 70,000,000	70	5
Inter-mediate	85	29,000,000	29	29
Bottom	10	1,000,000	1	1
Total	**100**	**$100,000,000**	**100**	**35**

[a] The preliminary estimate of sample size is computed by dividing the total balance by the sampling interval of $1,000,000. Refer to section 400 for additional information concerning sampling.

[b] The actual number of items tested in the top stratum may be fewer than the preliminary estimate of sample size because a top stratum selection may include more than one sample item. For example, if the implicit sampling interval is $1,000,000, a $2 million selection would include two of the sample items.

TESTING THE ITEMS

.06 The auditor determines the number of items to be tested at each location, and then selects and tests those items. For each line item/account the auditor should determine the total number of items to be tested, based on the applicable selection method and population, test materiality, and risk factors, as described in sections 480 and 495 E.

.07 The auditor should perform analytical and other procedures, as applicable, for both the locations selected and those not selected. Generally, the auditor should perform supplemental analytical procedures, including comparisons of locations with each other and with other years' information, for all locations, regardless of the selection method. When nonrepresentative selection is used, the auditor must apply appropriate substantive analytical procedures and/or other substantive procedures for locations not tested on-site, unless those locations are immaterial in total. Section 400 provides guidance on substantive and supplemental analytical procedures. Specific matters noted during the audit—for example, cutoff errors at one or more locations—may warrant increased or different audit procedures at locations not previously selected for on-site testing.

.08 In evaluating the result of a sample, the auditor estimates the effects, both quantitative and qualitative, on the financial statements taken as a whole, of any misstatements noted, as discussed in sections 480 and 540. In visiting selected locations, in addition to the issues concerning evaluation of samples in those sections, the auditor should exercise judgment and should apply the following additional procedures:

a. Determine if apparent misstatements are, in fact, misstatements that have not been corrected at some level in the entity.

b. Ask management to identify the cause of the misstatement.

c. Obtain evidence as to whether the same or similar types of misstatement exist at other locations (including locations not tested on-site). If the evidence is highly persuasive that the misstatement does not exist at other locations and the Audit Director concurs, the auditor may treat the effect on the entity the same as that on the location. (See paragraph 480.40 for a discussion of requirements for deciding whether evidence is highly persuasive.)

d. If the misstatement is not isolated to the location, determine whether there is evidence that the misstatement exists in other than a similar proportion throughout the entity. If such evidence exists, the auditor should obtain evidence of the incidence rate and should determine the effect on the entity; additional testing may be required. If no such evidence exists, the auditor should project the misstatement to the entity.

.09 In a nonrepresentative selection, the auditor should consider the possible effects of misstatements on locations not visited and determine whether additional audit procedures are required. Because the selection is not representative, the misstatements cannot be projected to the entity as a whole.

.10 The auditor should evaluate the sufficiency of audit procedures applied. The auditor should use judgment and should consider all relevant factors to determine whether the audit objectives are met, considering the specific circumstances.

[This page intentionally left blank.]

295 D - INTERIM SUBSTANTIVE TESTING OF BALANCE SHEET ACCOUNTS

.01 The auditor may consider performing significant substantive tests of balance sheet line items/accounts as of a date before the balance sheet date. If such interim tests are performed, the auditor should also apply audit procedures to the transactions during the "roll forward period" between the interim testing date and the balance sheet date (year end).

.02 Because evidence obtained as of the year end about an asset or liability balance provides a higher level of assurance than that obtained as of a prior or subsequent date, the audit risk generally increases as the length of the roll forward period increases. Although generally accepted auditing standards do not require moderate or low control risk to use interim testing, the auditor should consider inherent, control, and fraud risk in determining whether substantive tests of the roll forward period can be designed to provide a reasonable basis for extending the audit conclusions from the interim testing date to the year end.

.03 The additional audit procedures that should be performed during the roll forward period ordinarily increase the overall audit costs. However, by performing these procedures before the year's end, the auditor may be able to

- more quickly identify and address significant audit and accounting issues, such as problem areas and complex or unusual transactions, enabling the entity to correct misstatements or the auditor to modify the audit plan;
- complete the audit and issue the audit report earlier; and
- improve staff utilization and enable a smaller number of staff members to perform the audit by allocating the total audit hours over a longer period before the report issuance date.

.04 Generally, the auditor should not perform interim tests for an assertion with a high control or combined risk. In such instances, all substantive testing of balance sheet line items/accounts generally should be performed as of the year end. If the preliminary assessment of control and combined risk is moderate or low and exceptions are noted in the tests of controls, the auditor should use judgment, considering the nature, cause, and estimated effects of

the exceptions, to determine whether revisions of the preliminary control and combined risk assessments and audit plan are warranted.

.05 In determining whether to apply interim testing, the auditor should consider the following factors:

- **The assessment of inherent, control, and fraud risk:** The auditor should consider the risk of misstatement during the roll forward period, as well as all other relevant factors, including business conditions that may make management more susceptible to pressures, causing a misstatement of the financial statements. As combined risk (inherent and control risk) and fraud risk increase, so does the extent of the additional procedures that should be applied to the roll forward period, possibly making interim testing much more costly than testing the year-end balance. However, the auditor may be able to apply interim testing to certain assertions for which combined risk is assessed at lower levels while testing the other assertions as of the year end.

- **The anticipated comparability of the internal controls and the nature of the line item/account balances from the interim testing date to the year end:** To extend the audit conclusions from the interim date to the year-end date, it is essential that no significant changes in internal control occur from the interim date to the year-end date and that the line item/account balances consist of similar types of items at both dates.

- **The amount of the line item/account balance at the interim testing date in relation to the expected year-end balance:** A significant increase in the amount of the line item/account balance between interim and year-end dates would diminish the auditor's ability to extend the audit conclusions to the year end. In addition, applying substantive interim tests to a large line item/account balance may be inefficient if the year-end balance is expected to be lower than the balance at the interim date.

- **The length of the roll forward period:** The longer the roll forward period, the more difficult it is to control the increased audit risk. The roll forward period generally should not be longer than 3 months.

- **The anticipated level of transaction activity during the roll forward period:** Interim testing generally decreases in effectiveness and efficiency as the level of transaction activity during the roll forward period increases, particularly if there are large or unusual transactions during this period.

- **The ease with which substantive procedures can be applied to test the transactions during the roll forward period:** As the difficulty of such procedures increases, the efficiency of interim testing generally decreases.

- **The availability of information to test roll forward period activity using substantive analytical procedures, detail tests, or a combination of both:** If sufficient information is not available, interim testing is not appropriate.

- **The timing of the audit, staffing and scheduling requirements, and reporting deadlines:** Tight deadlines or the unavailability of necessary staff to perform audit procedures at the year's end may necessitate interim testing.

.06 In determining the timing of audit tests, the auditor should consider the relationships between line items/accounts that are affected by the same transactions. For example, if the auditor applies interim testing to inventory, the audit risk associated with inventory-related accounts payable, including cutoff matters, should be considered. The auditor may apply substantive procedures to each of the related line items/accounts as of the same interim testing date or may apply other procedures to obtain sufficient audit assurance.

.07 The auditor should document in the ARA (or equivalent) line items/accounts (and assertions, where applicable) to which interim testing is applied. The factors considered when concluding that the use of interim testing is appropriate should be documented in the GRA or equivalent.

[This page intentionally left blank.]

295 E - EFFECT OF RISK ON EXTENT OF AUDIT PROCEDURES

.01 The concepts of materiality and risk interrelate and sometimes are confused. The auditor determines materiality based on the users' perceived concerns and needs. The auditor assesses risk based on (but not limited to) knowledge of the entity, its business (purpose), applicable laws and regulations, and internal control.

.02 The auditor considers both materiality and risk in (1) determining the nature, timing, and extent of audit procedures and (2) evaluating the results of audit procedures. The evaluation of risk usually does not affect materiality. However, risk affects the extent of testing needed. The higher the auditor's assessment of inherent and control risk (combined risk), including fraud risk, the higher the required level of substantive assurance from the audit procedures. The discussion of consideration of risk in planning begins at paragraph 260.02. Consideration of risk in determining sample size is discussed in section 470.

.03 As an example, assume that the auditor is testing accounts receivable using dollar-unit sampling techniques described in section 480. Following are the pertinent data for this test:

- Accounts receivable total $2.5 million.
- Test materiality is $100,000.

If the auditor assesses combined risk as low, the sample size would be 25 items; if combined risk is assessed as high, the sample size would be 75 items. The increase in the assessment of risk caused the required sample size to triple with the same test materiality.

[This page intentionally left blank.]

295 F - TYPES OF INFORMATION SYSTEM CONTROLS

.01 As discussed in paragraph 270.04, the auditor should identify IS controls. Such controls should be tested by an IS auditor as described in section 300 and in accordance with the FISCAM or other appropriate methodology. IS controls can be classified into three types:

- general controls,
- application controls, and
- user controls.

GENERAL CONTROLS

.02 General controls are the policies and procedures that apply to an entity's overall computer operations and that create the environment in which application controls and certain user controls, which are control activities, operate. They are classified as

- **entitywide security management program** that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls;

- **access control** that limits or detects access to computer resources (data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure;

- **application software development and change control** that prevents unauthorized programs or modifications to an existing program from being implemented;

- **system software control** that limits and monitors access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system;

- **segregation of duties** that means having policies, procedures, and an organizational structure established so that one individual cannot control key aspects of computer-related operations and thereby conduct

unauthorized actions or gain unauthorized access to assets or records; and

- **service continuity control** to ensure that when unexpected events occur, critical operations continue without interruption or are promptly resumed and critical and sensitive data are protected.

Chapter 3 of the FISCAM has detailed guidance on evaluating and testing general controls.

.03 General controls are established at an (1) entity and/or installation/system level and (2) application level. For example, consider the following general controls related to security access:

- In evaluating general controls at the entity or installation level, the IS auditor considers security on an overall basis. For instance, the IS auditor may evaluate the entity's use of security access software, including its proper implementation.

- When evaluating general controls at the application level, the IS auditor reviews security controls that limit access to particular applications and related computer files. Thus, the IS auditor may focus on how security access software restricts access to payroll applications and related files (such as the employee master file and payroll transaction files) to authorized users.

- Finally, security is typically built into the application itself to further restrict authorized access. This security is usually accomplished by means of menus and other restrictions programmed into the application software. Thus, a payroll clerk may have access to payroll applications but may be restricted from access to a specific function, such as reviewing or updating payroll data on payroll department employees.

.04 The effectiveness of general controls is a significant factor in determining the effectiveness of application controls and certain user controls. Without effective general controls, application controls may be rendered ineffective by circumvention or modification. For example, the production and review of an exception report of unmatched items can be an effective application control. However, this control would be ineffective if the general controls permitted unauthorized program modifications such that certain items would be

inappropriately excluded from the report. Certain user controls are also affected by general controls. For example, a user control may be the comparison of manually calculated batch totals with computer-generated totals. Such a procedure would be ineffective if the general controls permitted unauthorized modifications of the program such that the program would print the desired batch totals without summarizing the detail.

APPLICATION CONTROLS

.05 Application controls are incorporated directly into individual computer applications to provide reasonable assurance of accurate and reliable processing. Application controls address three major operations:

- data input,
- data processing, and
- data output.

.06 FISCAM, in chapter 4, uses control categories that better tie in with the methodology used in the FAM. These categories relate to the financial statement assertions and are as follows.

- **Authorization control.** This category is most closely aligned with the financial statement accounting assertion of existence or occurrence and, therefore, focuses on the validity of transactions. Consequently, it includes controls designed to ensure that transactions are appropriately authorized and approved and represent economic events that actually occurred during a given period.

- **Completeness control.** This category directly relates to the financial statement accounting assertion on completeness and deals with whether all valid transactions are recorded. Also included in this category are reconciliation controls, which not only help detect misstatements relating to transaction completeness, but can also be used to identify the cutoff and summarization misstatements associated with both the existence or occurrence and completeness assertions.

- **Accuracy control.** This category most directly relates with the financial statement assertion on valuation or allocation, which deals with whether transactions are recorded at correct amounts. This control category, however, is not limited to valuation, and also includes controls

designed to ensure that transactions are properly classified and entered into the application correctly.

- **Control over integrity of processing and data files.** These application controls are not limited directly to one specific accounting application assertion, and if deficient could nullify other application controls and allow the occurrence of unauthorized transactions, as well as contribute to incomplete and inaccurate data.

USER CONTROLS

.07 User controls are manual comparisons of computer output (generally totals) to source documents or other input (including control totals). For example, a manual calculation of total hours worked may be reconciled to a corresponding computer-generated total from the payroll processing application. Where user controls are used, computer-generated information should be manually compared with reliable information prepared or verified independently of the computer.

.08 In certain circumstances, user controls may function independently of general controls. For example, a user control may be to manually check the accuracy and completeness of IS-computed transactions against manually prepared records. With the concurrence of the IS auditor, such control activities may be evaluated and tested without testing general controls.

295 G - BUDGET CONTROLS

.01 Budget controls are management's policies and procedures for managing and controlling the use of appropriated funds and other forms of budget authority. Budget controls are part of the internal controls covered in OMB's audit guidance. During planning, the auditor should assess related inherent risk and the control environment, risk assessment, communication, and monitoring and should obtain an understanding of the budget accounting system.

.02 Certain controls may achieve both financial reporting and other control objectives. Accordingly, to maximize efficiency, the auditor should coordinate the evaluation of budget controls with that of financial reporting, compliance, and operations controls, to the extent possible.

.03 Budget authority is authority provided by law to enter into financial obligations which will result in immediate or future outlays involving government funds (2 U.S.C. 622(2)). The Congress provides an entity with budget authority and may place restrictions on the amount, purpose, and timing of the obligation or outlay of such budget authority.

.04 The three forms of budget authority follow:

- **Appropriations** are the most common form of budget authority. An appropriation is an authorization by an act of the Congress that permits federal agencies to incur obligations and to make payments out of the Treasury for specified purposes. Appropriations do not represent cash actually set aside in the Treasury for purposes specified in the appropriation acts. Appropriations represent amounts that agencies may obligate during the period specified in the appropriation acts.

- **Borrowing authority** is statutory authority that permits federal agencies to borrow and obligate and expend borrowed funds (title 7 of the *GAO Policies and Procedures Manual*). Usually, the amount that may be borrowed and the purposes for which the borrowed funds are to be used are stipulated by the authorizing statute.

- **Contract authority** is statutory authority that permits obligations to be incurred before appropriations or in anticipation of receipts to be credited to a revolving fund or other account (offsetting collections). By definition,

contract authority is unfunded and must subsequently be funded by an appropriation or offsetting collections to liquidate the obligations incurred under the contract authority.

.05 Offsetting collections are collections of a business- or market-oriented nature and intragovernmental transactions. If, pursuant to law, they are deposited to receipt accounts and are available for obligation, they are considered budget authority and referred to as offsetting receipts. Contract authority and immediate availability of offsetting receipts for use are the usual forms of budget authority for revolving funds. Offsetting collections may also include reimbursements for materials or services provided to other government entities.

.06 Borrowing and contract authority are sometimes called "back door authority," which refers to any type of budget authority that is provided by legislation outside the normal appropriations process.

295 H - LAWS IDENTIFIED IN OMB AUDIT GUIDANCE AND OTHER GENERAL LAWS

.01 When identifying significant provisions of laws and regulations (see paragraph 245.02), the auditor should consider the following laws and regulations identified in OMB audit guidance in addition to any others that could have a direct and material effect on the financial statements and RSSI. Following each listed law is the subsection in FAM section 800 (under revision) that contains the compliance summary and audit program for that law.

- Antideficiency Act (codified as amended in 31 U.S.C. 1341, 1342, 1351, and 1517). (FAM section 803). Provisions: 31 U.S.C. 1341(a)(1)(A) and (C), and 31 U.S.C. 1517(a).

- Provisions Governing Claims of the United States Government as provided primarily in sections 3711-3720E of Title 31, Unites States Code (including provisions of the Debt Collection Improvement Act of 1996, Pub. L. No. 104-134, 110 Stat. 1321-358, which also is codified in various sections of 5 U.S.C., 18 U.S.C., 26 U.S.C., 31 U.S.C., and 42 U.S.C.). (FAM section 809). Provisions: 31 U.S.C. 3711, 31 U.S.C. 3717(a), (b), (c), (e), and (f), and 31 U.S.C. 3719.

- Federal Credit Reform Act of 1990, Pub. L. No. 100-508, 104 Stat. 1388-610 (codified in various sections of 2 U.S.C.). (FAM section 808). Provisions: 2 U.S.C. 661(b) and (e).

- Pay and Allowance System for Civilian Employees as provided primarily in Chapters 51-59 of Title 5, United States Code. (FAM section 812). Provisions: 5 U.S.C. 5332 and 5343 and 29 U.S.C. 206.

- Prompt Payment Act (codified as amended in 31 U.S.C. 3901-3907). (FAM section 810). Provisions: 31 U.S.C. 3902(a), (b), and (f) and 31 U.S.C. 3904.

OMB audit guidance lists the specific provisions for each law above that the CFO Act agency is expected to test at a minimum.

.02 The auditor should also consider whether any other general or entity-specific laws are significant laws for the audited entity, per FAM sections 245 and

802. The following are some general laws for which we have included in section 800 (under revision) a compliance summary for internal control testing and a compliance audit program. See FAM section 802 (Part II), General Compliance Checklist, and the referenced section for each law for internal control and compliance testing.

- Civil Service Retirement Act, 5 U.S.C. 8331 et. seq. (FAM section 813).

- Federal Employees' Compensation Act, 5 U.S.C. 8101 et. seq. (FAM section 816).

- Federal Employees Health Benefits Act, 5 U.S.C. 8901 et. seq. (FAM section 814).

- Federal Employees Retirement System Act of 1986. This becomes increasingly material each year as the number of employees covered by this act increases and those covered by the Civil Service Retirement Act decreases. We will include a new FAM section on the compliance summary and audit program for this act.

295 I - EXAMPLES OF AUDITOR RESPONSES TO FRAUD RISKS INVOLVING THE NATURE, TIMING, AND EXTENT OF AUDIT PROCEDURES

.01 As discussed in section 260, the auditor's response to assessed fraud risks should (1) have an overall effect on the conduct of the audit, (2) address fraud risks that relate to management override of controls, and (3)—for any fraud risks that relate to specific financial statement account balances or classes of transactions and related assertions—involve the nature, timing, and extent of audit procedures. This section provides examples of auditor responses in this third category—changing the nature, timing, and extent of audit procedures.

EXAMPLES OF AUDITOR RESPONSES TO FRAUD RISKS INVOLVING THE NATURE, TIMING, AND EXTENT OF AUDIT PROCEDURES

.02 Examples of auditor responses to fraud risks involving the nature, timing, and extent of audit procedures include the following:

- Inquire of management and other personnel involved in areas having fraud risks, such as risks related to any improper payments, to obtain their insights about those risks and whether and how controls mitigate those risks.

- Inquire of additional members of management, such as program directors or center directors, or other nonaccounting personnel to assist in identifying issues and corroborating other evidential matter.

- Use data mining or other computer-assisted audit techniques (such as Interactive Data Extraction and Analysis) to gather more extensive evidence about data contained in significant accounts. Such techniques can be used to select audit sample items from electronic files, sort items with specific characteristics (to perform substantive analytical procedures or make a nonrepresentative selection), or test an entire population.

- Inspect, or observe physical counts of, tangible assets, such as property, plant, and equipment and certain inventories, for which other procedures might otherwise have been sufficient.

- Conduct surprise or unannounced procedures, such as inventory observations or cash counts on unexpected dates or at unexpected locations.

- Make inquiries of major suppliers or customers in addition to obtaining written confirmations, request confirmations of a specific individual within an organization, or request confirmation of additional or different information.

- Where a specialist's (see section 650 and AU 336) work is particularly significant, perform additional procedures related to some or all of the specialist's methods, assumptions, or findings to evaluate whether the findings are unreasonable, or engage another specialist to do that.

- Perform additional or more focused tests of budget to actual variances and their underlying causes.

- Perform targeted tests of the timing of cost/expense recognition.

- Request that physical inventory counts be made on, or closer to, the date that the reporting period ends.

- If fraud risks relate to an interim period, perform audit tests that are focused on transactions that occurred in that interim period (or throughout the reporting period).

- Test a larger sample of disbursement transactions for validity.

- Perform substantive analytical procedures that are more detailed by location, program, month, or other category (for example, analyzing specific credit lines in an allowance for loan losses, rather than the portfolio as a whole) or that use more precise techniques (for example, regression analysis).

- Discuss with other auditors who are auditing the financial statements of one or more agency components the extent of work necessary to address fraud risks resulting from intragovernmental transactions and activity among those components.

ADDITIONAL EXAMPLES OF AUDITOR RESPONSES TO FRAUD RISKS RELATED TO MISSTATEMENTS ARISING FROM FRAUDULENT FINANCIAL REPORTING

.03 The following paragraphs provide additional examples of auditor responses to fraud risks related to misstatements arising from fraudulent financial reporting in the areas of (1) management's estimates, (2) revenue recognition, and (3) inventory quantities. These example responses involve the nature, timing, and extent of audit procedures.

Management's Estimates

.04 Fraud risks might relate to management's development of accounting estimates. These risks might affect various accounts and assertions, such as valuation and completeness of liabilities related to insurance and credit programs, pensions, postretirement benefits, and environmental cleanup. These risks might also relate to significant changes in assumptions for recurring estimates. Further, because estimates are based on both subjective and objective factors, bias might exist in the subjective factors.

.05 Examples of procedures that the auditor might perform in response to fraud risks related to management estimates include the following:

- Gather additional information about the entity and its environment to assist in evaluating more extensively the reasonableness of management's estimates and underlying judgments and assumptions, focusing on more sensitive or subjective aspects.

- Perform a more extensive retrospective review of management judgments and assumptions applied in estimates made for prior periods, such as analyzing each significant judgment and assumption in light of the events that occurred subsequently and identifying reasons for any differences. Consider whether these reasons should affect the current period's estimates.

- Use the work of a specialist to evaluate management's estimate, or develop an independent estimate to compare to management's estimate.

Revenue Recognition

.06 Revenue recognition is affected by the particular facts and circumstances and sometimes—for example, for certain government corporations—by accounting principles that can vary by type of operations. Hence, where revenue is (or is expected to be) material, the auditor should be familiar with the applicable criteria for revenue recognition by a federal government entity, and the audit procedures should reflect the auditor's understanding of the entity and its environment, including the composition of revenue, specific attributes of the revenue transactions, and specific entity considerations.

.07 Examples of procedures that the auditor might perform in response to fraud risks related to improper revenue recognition include the following:

- Perform substantive analytical procedures related to revenue that are based on more precisely developed expectations, such as comparing revenue between the current year and expectations based on prior fiscal years, by location, program, and month, or that establish the limit (see paragraphs 475.04-.05) at a lower percent of test materiality. Audit techniques such as regression analysis might be helpful in performing these procedures.

- Inquire of the entity's personnel, including its general counsel, about any revenue-related transactions near the end of the reporting period and their knowledge of any unusual terms or conditions that might be related to those transactions.

- Confirm with customers and other appropriate parties the relevant contract terms and the absence of side agreements that might influence the appropriate accounting.

- Physically observe goods being shipped or readied for shipment (or returns awaiting processing) at one or more locations at the end of the reporting period and perform appropriate sales and inventory cutoff procedures.

- Where revenue transactions are electronically initiated, processed, and recorded, expand control tests related to these transactions.

Inventories

.08 Examples of procedures that the auditor might perform in response to fraud risks related to inventories include the following:

- Review the entity's inventory records to identify locations, items, or issues that warrant specific attention during or after the physical inventory count. As a result, the auditor might decide to observe inventory counts at some locations on an unannounced basis or to request that physical inventory counts be made at all locations on the same date and on a date that is on, or closer to, the date that the reporting period ends.

- Perform additional inventory observation procedures, such as more rigorously examining the contents of boxed items, the manner in which the inventory is stacked (to identify hollow squares or other issues) or labeled, and—using the work of a specialist, if needed—the purity, grade, and concentration of inventory substances such as specialty chemicals.

- Perform additional tests of physical inventory count sheets or tags, and retain copies of these documents to minimize the risk of subsequent alteration or inappropriate extension and summarization of the inventory.

- Perform additional procedures focused on the quantities included in the priced inventory to further test the count quantities—such as comparing quantities for the current period with those for prior periods by inventory category, location, or other criteria, or comparing count quantities with perpetual records.

- Use computer-assisted audit techniques (such as Interactive Data Extraction and Analysis) to test the extension and summarization of the physical inventory counts—such as sorting by tag number to test tag controls or by item number to test for item omission or duplication—and to test for unusual quantities and cost amounts.

- When performing substantive analytical procedures related to inventories, establish the limit (see paragraphs 475.04-.05) at a lower percent of test materiality.

ADDITIONAL EXAMPLES OF AUDITOR RESPONSES TO FRAUD RISKS RELATED TO MISSTATEMENTS ARISING FROM MISAPPROPRIATION OF ASSETS

.09 Additional examples of auditor responses to fraud risks related to misstatements arising from misappropriation of assets involving the nature, timing, and extent of audit procedures include the following:

- Use information on any improper payments, including information resulting from the agency's review of programs and activities under the Improper Payments Information Act of 2002, to develop and perform audit procedures that are focused on specific vulnerable areas.

- For benefit programs, expand the extent of participant eligibility testing, including unannounced visits to intake centers or work sites to test the existence and identity of participants, or observe benefit payment distribution to identify "ghost" participants or use confirmation requests to test the existence of program participants. Data mining can be used to search for duplicate payments, ineligible or ghost participants, and other issues.

- For particular assets that are highly susceptible to misappropriation, obtain a more comprehensive understanding of internal controls related to preventing

and detecting such a misappropriation and expand the tests of those controls, and physically inspect those assets at or near the end of the reporting period.

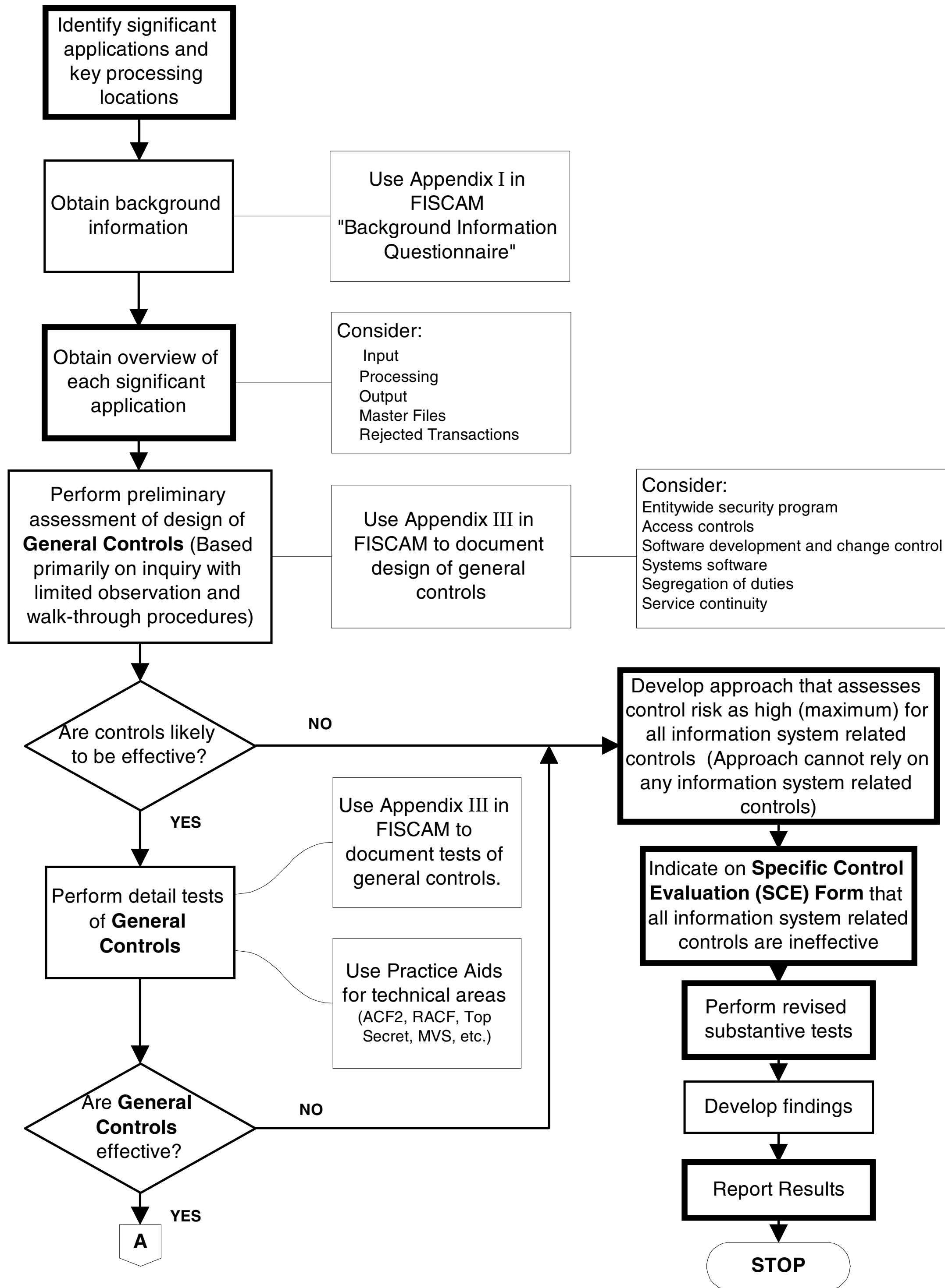
- Assign higher levels of control risk to specific locations that have higher fraud risks (such as when large quantities of assets that are particularly susceptible to such risks are present at some locations) and modify audit procedures at those locations.

- When performing substantive analytical procedures related to assets that are particularly susceptible to misappropriation, establish the limit (see paragraphs 475.04-.05) at a lower percent of test materiality.

295 J - STEPS IN ASSESSING INFORMATION SYSTEM CONTROLS

.01 As discussed in section 260, the following are the steps the auditor and the IS auditor generally follow in assessing IS controls in a financial statement audit. However, the audit team may decide to test the effectiveness of the general controls even if they are not likely to be effective, or the team may decide to review application controls even though general controls are not effective. The team may decide to do this to be able to make better recommendations on how to fix weak controls.

Steps in Assessing Information System Controls In a Financial Statement Audit



Steps in Assessing Information System Controls In a Financial Statement Audit -- (continued)