

SECTION 1
ADDENDUM C
CONDUCTING INTERNAL CONTROL REVIEWS

Internal Control Reviews include all high risk areas in each event cycle. They are usually much more time-consuming and paper-intensive than Alternative Internal Control Reviews. Therefore, they are to be used sparingly.

The Department has decided that Internal Control Reviews (ICR) are to be done on all controls or program areas considered to be of high risk. As discussed later in this handbook, since an ICR requires a description of all event cycles and analysis of control objectives and techniques, testing is normally very detailed and extensive. When the level of risk for controls or program areas is considered to be low, the Department has decided that an Alternative Internal Control Risk is appropriate because it is generally less paper intensive and more cost effective and efficient. For program areas considered to be medium risk, it is management's discretion as to whether the ICR or AICR is more appropriate; the decision to use the ICR or AICR should be based on the visibility of the program, the dollar impact of the program on outside entities (public or governmental), etc.

Suggested steps for conducting ICRs are listed below.

START THE EVALUATION

Plan the Evaluation

The ICR should be carefully planned to gain managerial support and to ensure that objectives are accomplished. The planning process should include the following tasks.

- **Determine scope and objectives.** Consider whether the purpose of the AICR is to perform a comprehensive review of controls over all the high risk areas or if it is to perform a limited review of one aspect of the component.
- **Assign staff.** The team members selected should be knowledgeable of the program area, have analytical skills, and be trained in conducting control evaluations. Ideally, team members should be selected from within the responsible program office or from an independent "program-evaluation" office. The number of reviewers should be based on the complexity and scope of the review.
- **Allocate staff resources and establish timeframes.** It is helpful to identify the minimum and maximum amount of staff resources to be used for completing each task. The final planned completion date should be set with interim planned completion dates for each review task.

Component Survey

The next step in the assessment process is to survey the component to be reviewed. The survey is primarily a fact-finding and data-gathering exercise to establish the framework in which the component operates. It includes reviewing authorizing legislation, implementing regulations, policies and procedures, planning and budget documents, organizational charts, and other pertinent documents and records. It also includes reviewing audit reports, results of internal reviews, and similar evaluations. The survey provides the input for the steps that follow. If a survey has been previously conducted, the reviewer should check to see if the survey is still accurate.

Analysis of the General Control Environment

The purpose of analyzing the general control environment is to determine if management's attitude is conducive to a strong internal control system. The analysis of the general control environment will provide the reviewer with a preliminary opinion about the effectiveness of specific controls. If an analysis has been previously completed, check to see if it is still accurate and update as necessary. (Use Worksheet in Exhibit 1 for this analysis).

The factors that influence the general control environment are:

- Organization;
- Delegation of authority;
- Policies and procedures;
- Personnel;
- Planning, Budgeting, and Accounting; and
- Reporting.

Analysis of Information Technology

If the component contains an IT application, it should be analyzed to determine if IT application controls should be reviewed. This review of IT can be a separate review. An IT application should be included if it contains any of the following characteristics.

- Processes information used for significant management decisions;
- Calculates or records amounts owed by or to the government;
- Maintains balances or other records used to control government resources;
- Maintains or processes information necessary for effective and efficient program operation; or
- Maintains or processes sensitive information.

NOTE: Section 3, Chapter 3, Executing ICR for Information Systems and IT Programs, of this handbook provides additional details on this process.

DEFINE CONTROL SYSTEMS

Identify and Document Event Cycles

An event cycle is a series of related steps that constitute a distinct and separate process or activity within a component. Each program or administrative component of a bureau contains one or more event cycles that help achieve the goals of the component.

In general, components can be comprised of either process-related sets of event cycles, as in administrative-type components, or program sets of event cycles. For example, the cash management administrative component of a bureau normally includes billing, collecting, depositing, procuring, and disbursing event cycles. By contrast, most program components normally include planning, budgeting, executing, reporting, and administrative event cycles.

Some components, such as concessions management, may be described as either an administrative or program component and, accordingly, may be segmented into administrative or program event cycles. It is up to the reviewer to determine which type best fits the component being reviewed.

An important step in the review process is to first identify and then list all the event cycles of the component. The next step is to develop a thorough understanding of how each event cycle functions. If a detailed description of the event cycle does not already exist, then documentation should be prepared using flowcharts and/or narrative descriptions. This detailed description should be retained as part of the ICR documentation.

Background information necessary for creating such documentation may be obtained through interview, observation, or existing records such as mission and function statements. Documentation of the event cycle should be sufficient to provide an in-depth understanding of the objectives and operations of every cycle.

Identify and Document All Risks

After listing the event cycles, the potential risks involved within each event cycle must be identified. The reviewer should categorize the identified risks within each cycle as high, medium, or low. The impact of each risk (the probability of its occurrence and the severity of its consequences) should be considered. High risks are those which could prevent the event cycle from achieving its objective or result in substantial loss of government resources.

The reviewer would then determine, based upon knowledge of the activity and the objective of the event cycle, which risks are high.

Identify and Document Control Objectives

Control objectives are what you want to achieve. Specifically, control objectives are the desired goals for a specific event cycle that reduce the potential for fraud, waste, and abuse or ensure the efficiency, effectiveness, and economy of operations within the event cycle. These objectives should correspond to the risks identified for the event cycle and set forth the specific goals the control system is to meet.

Setting control objectives involves turning the potential risk into a goal. To identify a control objective, ask what needs to happen in order to avoid a specific risk. The reviewer should state what the objective will achieve and how it will be determined whether the objective was achieved.

If the component being reviewed does not have control objectives, the reviewer should develop the control objectives during the review in order to proceed to identifying and documenting the control techniques.

Identify and Document Control Techniques

Control techniques are a series of carefully constructed checks and balances designed to provide reasonable assurance that the control objectives are met in an efficient and effective manner. Control techniques should be observable and cost effective. Examples of control techniques include passwords to limit access to databases, written delegations of authority, technical reports, documentation of processes and procedures for carrying out program and administrative activities, periodic supervisory reviews, comparisons of actual results to planned results, and segregating sensitive duties among several individuals.

When developing control techniques, it is crucial to identify the relationship between the techniques to determine if the controls are operating as planned and are sufficient to provide reasonable assurance of achieving the control objectives.

Compare Control Systems to the GAO Control Standards

The GAO control standards (**web site address www.gao.gov**) define the minimum level of quality acceptable for an internal control system. These standards apply to all operations and functions except development of legislation, rulemaking, or discretionary policymaking. The five GAO standards for internal control are: (1) Control environment; (2) risk assessment; (3) control activities; (4) information and communications; and (5) monitoring. These standards define the minimum level of quality acceptable for internal control in government programs and administrative operations and provide the basis against which internal control is to be evaluated. The standards apply to all aspects of an agency's operations—programmatic, financial, and compliance.

NOTE: The term internal control as used in the GAO standards is synonymous with the term management control as it was used in the prior version of OMB Circular A-123.

The GAO standards provide a general framework for internal controls. Agency/bureau management is responsible for developing the detailed policies, procedures, and practices to fit their operations, and ensuring that internal controls are built into and are an integral part of operations. A more detailed description of the standards follows.

- **Control Environment.** Management and employees should establish and maintain an environment throughout the organization that sets a positive and supportive attitude toward internal control and conscientious management.
- **Risk Assessment.** Internal control should provide for an assessment of the risks the agency faces from both external and internal sources. Risk assessment is the identification and analysis of relevant risks associated with achieving the objectives, such as those defined in strategic and annual performance plans developed under the GPRA, and forming a basis for determining how risks should be managed.
- **Control Activities.** Internal control activities help ensure that management's directives are carried out. The control activities should be effective and efficient in accomplishing the Department's control objectives. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They also help ensure actions are taken to address risks. Control activities include approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities along with supporting documentation. Examples of control activities include:
 - Top level reviews of actual performance;
 - Reviews by management at the functional or activity level;
 - Management of human capital;
 - Controls over information processing;
 - Physical control over vulnerable assets;
 - Establishment and review of performance measures and indicators;
 - Segregation of duties;
 - Proper execution of transactions and events;
 - Accurate and timely recording of transactions and events;
 - Access restrictions to and accountability for resources and records; and
 - Appropriate documentation of transactions and internal control.
- **Information and Communications.** Information should be recorded and communicated to management and others within the entity who need it and in a form and within a timeframe that enables them to carry out their internal control and other responsibilities.

- Monitoring. Internal control monitoring should assess the quality of performance over time and ensure that the findings of audits and other reviews are promptly resolved.

REVIEW THE SYSTEM DESIGN

An assessment of a system of internal controls is based on a documented understanding of the system. Information obtained during the survey of the component and documentation of the control system should be studied. This part of the ICR should focus on the adequacy of the control objectives and the design of the control techniques. During this process, the reviewer should answer at least the following questions.

Adequacy of control objectives: An agency must review sufficient controls to assure that systems and applications are designed to operate effectively, provide confidentiality, integrity, availability and protect information from loss, misuse and unauthorized access or modification.

Adequacy of control techniques: Control techniques must determine and gain a high level indication that the system and the information are adequately secured. Management, Operational and Technical controls should all be included in the assessment.

- Have complete, logical, and applicable control objectives been established?
- Do existing controls appear sufficient to manage the risks and satisfy the control objectives?
- Do existing controls appear excessive for the risks and control objectives specified?
- Can or should other controls be used to either reduce risk or improve the efficiency of the system?

The answers to these questions will lead the reviewer to a judgment about the system's theoretical strengths and weaknesses. This, in turn, enables the reviewer to focus on the appropriate areas to be examined during the testing phase.

TEST THE CONTROL SYSTEM

Testing verifies the effectiveness of control techniques in operation by determining if they are, in fact, operating as intended, meeting the control objectives, and reducing risks. By testing, the responsible official can quickly validate whether:

- Prescribed procedures are performed in accordance with instructions;
- Procedures are performed by personnel having no incompatible duties;
- Actual transactions processed in the operation are in fact those authorized for the group; and
- Actual operations are conducted in accordance with the control objectives and techniques which have been devised for the component.

The focus of testing should be upon high risk areas and those areas of inadequate internal control system design. Testing consists of the following steps.

Select Controls to be Tested

It is both impractical and unnecessary to test all control techniques. The control techniques to be tested should be those that contribute most to achieving the control objectives or managing the risk. A control should be eliminated from testing when: (1) The technique does not meet the control objective or manage the risk because it is poorly designed, unnecessary, duplicative, or is not performed in a timely manner; and (2) the cost of testing exceeds the value of the technique being tested. If a technique is excluded from testing, the reasons supporting this decision should be recorded.

Select Test Methods

Testing methods include:

- Document analysis – reviewing existing records, completed forms, or other documentation;
- Transaction testing – entering and processing transaction data through the system or by tracing transactions through the system;
- Observation – watching the performance of specific control technique; and/or
- Interview – eliciting information from the personnel who perform the control technique.

Tests should not be limited to information obtained through interviews, but interviews should be used to supplement document analyses and/or observation. One or more methods of testing may be combined during the test.

The Automated Assessment Approach discussed in detail in Addendum A may also be used here. Please refer to Addendum A for additional information.

Determine Amount of Testing

It is unrealistic to observe every time a control is used or review 100% of the records at all locations. The reviewer must select the organizations and locations where the tests will be conducted and select a sample for each control to be tested.

Plan Data Collection

Accurate recording of test results is an extremely important part of the testing process. A data collection plan assists in determining how to record the test results. For example, interview guides should be used to ensure that all areas of concerns are discussed.

Conduct the Tests

While conducting the tests, the sample plan should be followed unless it is determined that it is necessary to revise the scope or size of the sample based on the results of the initial sample. Consider increasing the sample size if the initial tests provide mixed results. When possible, retain copies of authorizing documents or other physical evidence that control techniques are working.

A control is not effective when the assessment determines it is not adequately designed or when it is reviewed and determined that it is not functioning effectively. There is a control gap when a control does not exist for a given assertion, when a control does not adequately address a relevant assertion, or a control is not operating effectively. Reviewers should always determine that other compensating controls do not exist that would mitigate the risk.

NOTE: Watch for compensating controls. Sometimes a control technique will appear to be weak or not operating. In such a case, determine if personnel are compensating for the shortcomings by using informal control mechanisms. If informal control mechanisms are being used, evaluate and document them during the testing.

Analyze Test Results and Develop Conclusions

The tests of specific control techniques must be analyzed to determine if the degree of compliance with control techniques is adequate. It is important to remember that usually several control techniques are utilized to meet a control objective or manage a risk. Accordingly, the failure to substantially comply with one individual control technique does not necessarily result in a failure to meet the control objective or manage a risk.

The test results should then be discussed with managers responsible for operating the control techniques at the location or organization that was reviewed. These discussions will: (1) Communicate the results of the tests and any conclusions drawn; (2) seek agreement on those conclusions, and (3) elicit recommendations from the managers on any necessary corrective actions. Such discussions are best held as soon as the testing and related analyses of results are completed.

Develop Plans for Corrective Action

The primary purpose of the control assessment process is to assist managers in identifying and correcting weaknesses. When a weakness is found, a decision must be made to institute new controls, improve existing controls, or accept the risk inherent in the weakness. In many cases

the appropriate action is apparent but in other cases further analysis may be necessary before a plan for corrective action can be made. Selecting corrective actions involves creating a strategy for achieving the control objectives. The actions selected should use the least amount of dollar and personnel resources possible and ensure the achievement of the control objectives or results.

The following information should be completed while preparing corrective action plans (Refer to Chapter 4, Developing and Implementing Corrective Actions, for detailed requirements).

- Summary Description of the Weakness/Deficiency
- Year First Identified
- Target Correction Date
- Accountable Official
- Funding/Resources Required to Resolve the Weakness/Deficiency
- Summary of Corrective Actions
- Quarterly Corrective Actions
- Metrics

REPORT THE RESULTS

Control assessment results for each component should be summarized in a report. The report should identify control weaknesses and describe plans for corrective action. Since the report forms the basis for the certification required by FMFIA, it should provide the bureau head and program assistant secretary with sufficient assurance that the review was conscientiously performed and accurately reflects the condition of internal controls.

The report should contain all control weaknesses which are significant to the next higher organizational level, regardless of the process through which the weaknesses were identified. All sources of information on the status of controls, such as audit reports, management reviews, and routine management reports, are to be considered in identifying control weaknesses. The transmittal memorandum should describe: (1) Risks that the evaluation focused on; and (2) testing conducted, locations, controls techniques tested, and type and amount of testing.

The report should be submitted to the official designated as responsible for component controls and their evaluation. After review by the responsible official, the report is to be transmitted to the bureau ICC for approval by the bureau head. The report must be approved by the bureau head and appropriate program assistant secretary and submitted to PFM with a copy to the OIG.

DOCUMENT THE EVALUATION

Documentation is written material explaining the operation of the control system and the conduct of an internal control assessment. GAO specific control standards require that all internal controls and all transactions and other significant events are to be clearly documented, and the documentation is to be readily available for examination. In addition, responsible officials should prepare and maintain sufficient documentation to evidence the conduct of an internal

control assessment and the basis for the results and conclusions reached. This documentation should include written evidence concerning:

- The officials participating in the review;
- The risks reviewed;
- The controls examined;
- The extent and type of control tests performed;
- The analysis of the tests conducted;
- A description of any weaknesses found;
- The actions recommended to correct the weaknesses; and
- The responsible official.

System documentation provides a means of communicating information on the operation of the control system and it serves as a standard to measure the operation of the control system. It further provides information necessary for supervisory or other review and serves as a basis for training new personnel. Evaluation documentation provides evidence that an internal control assessment was performed and provides support for the reasonable assurance determination. It serves as the basis for supervisory review and quality control while assisting in subsequent assessments.

How much documentation is enough? Sufficient system documentation answers why the system was designed, what the system does, and how the system operates. Sufficient evaluation documentation tells the reviewer who did what, what were the results, and why were actions taken.

NOTE: Sufficient documentation should not involve an inordinate amount of paper. However, when testing financial reporting internal controls, sufficient documentation must be available to demonstrate the bureau's assessment.