Additional Help: 591
File Name: 591sab_121701_cd26
Last Revised: 12/17/2001

This document consists of two parts: Appendix A, Recipient
Control Environment Assessment Checklist, and Appendix B,
Non-U.S.-Based Organizations Assessment Guide.

<div align="right">**APPENDIX A**</div>

RECIPIENT CONTROL ENVIRONMENT ASSESSMENT CHECKLIST

Control Environment:

Control environment risk factors incorporate management's
attitude, awareness, and actions concerning an
organization's control environment. It is important that
the individual performing the risk assessment obtain
sufficient knowledge of the control environment to
determine whether the collective effect of these factors
establishes, enhances, or mitigates the effectiveness of
the specific control techniques. In making this
determination, the reviewer should consider the following
factors and their effect on the organization's internal
controls. The specific conditions listed below may
indicate the presence of control environment weaknesses.

A.   Management's Philosophy and Operating Style:

   •   Management lacks concern about internal controls
        and the environment in which specific controls
        function.

   •   Management demonstrates an aggressive approach to
        risk taking and accounting policies.

   •   Management is slow to respond to crisis
        situations in both operating and financial areas.

   •   Management uses unreliable and inaccurate
        information to make business decisions.

<div align="right">1</div>

- Unexpected reorganization or replacement of management staff or consultants occurs frequently.

- There is a high turnover of management personnel.

- Management is overly optimistic regarding performance of programs and activities, and financial estimates consistently prove to be significantly overstated or understated.

- Management is not able to adapt to new or untraditional roles required to meet the changing needs of the organization.

- Communication and feedback systems within the organization are inadequate.

- The organization's financial sustainability is questionable.

B.   The Entity's Organizational Structure:

- The organizational structure is inappropriate for the entity's size and complexity.

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

- Delegation of responsibility and authority is inappropriate, and the number of supervisors is inadequate or supervisors are inaccessible.

- Inexperienced and/or incompetent accounting personnel are responsible for transaction processing.

- 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 officials of the organization to obtain financial or other benefits on the basis of decisions made or actions taken in an official capacity.

- Organizational conflict of interest exists and is an accepted practice.

- The organization is highly centralized with minimal review provided by top management.

- The organization is highly decentralized with minimal review provided by branch managers or other sub-organization management.

- The organization has many subrecipients or branches in many in numerous geographical locations.

C. Methods of Assigning 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.

- Employee job descriptions do not adequately describe specific duties, responsibilities, reporting relationships, and constraints.

D. Management's Monitoring of Performance:

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

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

- Management's follow-up action is not timely or inappropriate in response to communications from external parties, including complaints, notification of errors in transactions with parties, and notification of inappropriate employee behavior.

E. Human Resources Policies and Practices:

- Human resources policies for hiring, retaining, and rewarding capable people are inadequate.

- Standards and procedures for hiring, promoting, transferring, retiring, and terminating personnel are insufficient.

- Training programs do not offer employees the opportunity to improve their performance, encourage their advancement, or provide a vehicle for addressing employee or organizational weaknesses relative to new laws, regulations, and policies.

- Written job descriptions and reference manuals are inadequately maintained.

- The channels of communication for employees reporting suspected improprieties are inappropriate.

- Policies on employee supervision are inappropriate or obsolete.

- Policies and procedures do not provide for employee empowerment nor do they encourage and support risk taking and initiatives for performance improvement.

F. Budget Control:

- Little or no guidance material and instructions are available to provide direction to those preparing the budget.

- 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 or limited.

- Management is not involved in determining when, how much, and for what purpose expenditures can be made.

- Actual expenditures are not periodically compared to budgets.

G. Compliance with Laws and Regulations:

- Management is unaware of 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.

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

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

- The organization and/or its subrecipients are receiving USAID funding for the first time and are not familiar with our compliance requirements.

H. Changing Conditions:

- 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.

- Consideration is not given to designing new or alternative controls in response to changing conditions.

- Management is unresponsive to changing conditions.

Risk Assessment Checklist:

Once the reviewer has developed a reasonable understanding of the organization's control environment, the following risk assessment checklist should be completed. The checklist details the specific control techniques that should be reviewed in order to determine the risk level for each recipient of USAID funds that expends less than $300,000 per fiscal year and is not required to have an annual audit. The checklist should be completed for each applicable recipient and updated on a periodic basis.

I. AUTHORIZATION

Authorization controls are designed to provide reasonable assurance that transactions, events from which they arise, and procedures under which they are processed are authorized in accordance with laws, regulations, and management policy. Typical authorization controls include:

1. Documented policies establish events or transactions that the organization is authorized to engage in by law, regulation, or management policy.

2. Documented policies and procedures exist for processing transactions in accordance with laws, regulations or management policy.

3. Master files include only authorized employees, customers, or suppliers.

II. APPROVAL

Approval controls are designed to provide reasonable assurance that appropriate individuals approve recorded transactions in accordance with management's general or specific criteria. Typical approval controls include:

1. Specific transactions are approved by persons having the authority to do so in accordance with established policies and procedures.

2. Transactions are compared with predetermined expectations, and exceptions are reviewed by someone authorized to approve them.

3. Transactions are compared with approved master files before approval or acceptance, and exceptions are reviewed by someone authorized to approve them.

4. Key records are matched before a transaction is approved (matching purchase order, receiving report, and vendor invoice before the invoice is approved for payment).

5. Prior to acceptance, changes to data in existing files are independently approved, evidenced by documentary approval of input before processing.

III. Segregation of Duties

Segregation of duties controls are designed to reduce the opportunities for someone to perpetrate and/or conceal errors or irregularities in the normal course of their duties. Typical segregation of duties controls include:

1. The individual responsible for the cash receipts function does not sign checks or reconcile the bank accounts, and is not responsible for noncash accounting records such as accounts receivable, the general ledger, or the general journal.

2. The person receiving cash does not have the authority to sign checks and reconcile bank accounts and does not have access to accounting records other than cash receipts.

3. Different individuals are responsible for purchasing merchandise or services, receiving merchandise or services, and approving vouchers.

4. Different persons prepare checks, sign checks, reconcile bank accounts, and have access to cash receipts.

IV. Design and Use of Records

The purpose of controls over the design and use of records is to help provide reasonable assurance that transactions and events are properly recorded.

1. Pre-numbered forms are used to record all of an organization's transactions, and accountability is maintained for the sequence of all numbers used.

2. Receiving reports, inspection documents, etc., are matched with billing notices or other documents used to record delivered orders and related liabilities to provide assurance that only valid transactions are recorded.

3. Transaction documents, such as vendor invoices and shipping documents, are date stamped and tracked to ensure that they are recorded on a timely basis.

4. Source documents are canceled after processing to provide assurance that the same documents will not be reused and will not result in recording transactions more than once. Also, only original documents are used to process transactions.

V. SAFEGUARDS OVER ACCESS TO AND USE OF ASSETS AND RECORDS

Access controls are designed to protect assets and records against physical harm, loss, misuse, or unauthorized alteration. These controls restrict unauthorized access to assets and records. Typical access controls are:

1. Cash receipt totals are recorded before cash is transmitted for deposit.

2. Secured facilities are used when appropriate, and access to critical forms and equipment is limited to authorized personnel.

3. Access to programs and data files is restricted to authorized personnel.

4. Assets and records are protected against physical harm.

5. Incoming and outgoing assets are counted, inspected, and received or given up on the basis of proper authorization in accordance with established procedures.

6. Procedures are established to provide reasonable assurance that current files can be recovered in the event of a computer failure.

7. Access to critical forms and records is restricted.

VI. INDEPENDENT CHECKS

Controls in this category are designed to provide independent checks on the validity, accuracy, and completeness of processed data. The following procedures are typical of this category of controls:

1. Calculations, extensions, additions, and accounting classifications are independently reviewed.

2. Assets on hand are periodically inspected and counted, and the results are compared with asset records.

3. Subsidiary ledgers and records are reconciled to the general ledger.

4. The organization promptly follows-up on complaints from vendors, customers, employees, and others.

5. Management reviews performance reports.

6. Data from different sources are compared for accuracy and completeness (the cash journal entry is compared with the authenticated bank deposit slip).

7. Actual operating results are compared with approved budgets, and variances are explained.

VII. VALUATION OF RECORDED AMOUNTS

Controls in this category are designed to provide assurance that assets are valued at appropriate amounts. Typical valuation controls are:

1. Periodically, the condition and marketability of assets are evaluated (for example, accounts

receivable are periodically evaluated for
collectibility).

2.   Recorded data are compared with information from
      an independent third party (for example, recorded
      cash is reconciled to bank statements).

3.   Assessed values, such as independent appraisals
      of assets, are compared with the accounting
      records.

VIII. SUMMARIZATION OF ACCOUNTING DATA

Controls in this category are designed to provide assurance
that transactions are accurately summarized and that any
adjustments are valid. Typical controls in this category
include:

1.   The sources of summarized data are compared with
      the underlying subsidiary records and/or
      documents before the data are accepted for
      inclusion in summarized records and reports.

2.   Procedures are followed to check the completeness
      and accuracy of data summarization, and
      exceptions are reviewed and resolved by
      authorized persons.

IX. ASSETS AND LIABILITIES

Controls in this category are designed to provide assurance
that (1) the organization owns recorded assets, with the
ownership supported by appropriate documentation; (2) the
organization has the rights to its assets at a given date;
and (3) recorded liabilities reflect the organization's
legal obligations at a given date. The following
procedures are typical for this category of controls:

1.   Policies and procedures are documented for
      initiating transactions and for identifying and
      monitoring those transactions and amounts
      requiring attention relative to ownership issues.

2.   Policies and procedures are documented for
      initiating and monitoring transactions and
      amounts related to liabilities.

3.   Significant transactions require the approval of
      senior management.

4.   Reported results and balances are compared with
      plans and authorizations.

X. PRESENTATION AND DISCLOSURE

Controls in this category are designed to provide assurance
that (1) accounts are properly classified and described in
the financial statements; (2) the financial statements are
prepared in accordance with applicable accounting
principles; and (3) footnotes contain all information to be
disclosed. The following procedures are typical of this
category of controls:

1.   Policies and procedures are documented for
      accumulating and disclosing financial information
      in the financial statements by appropriate
      personnel and in accordance with the terms of the
      agreement. Responsibility is assigned to
      specific individuals.

2.   Policies and procedures are documented for
      preparing financial statements by authorized
      personnel having sufficient experience and
      expertise to ensure compliance with applicable
      accounting principles.

3.   Policies and procedures are documented for
      properly classifying and describing financial
      information in the financial statements.

4.   Reports are periodically substantiated and
      evaluated by supervisory personnel. Procedures
      have been implemented to detect errors and
      omissions and to evaluate recorded balances.

5.   A written chart of accounts containing a
      description of each account is used. Journal
      entries are prepared, reviewed, compared with
      supporting details where necessary, and approved
      each accounting period.

6.   Appropriate processing procedures are used,
      including control or batch totals; written cutoff
      and closing schedules are also used.

7.   The same chart of accounts is used for both
      budgeting and reporting, and variances between
      actual and planned results are analyzed.

SUGGESTED APPROACH

NON-U.S.-BASED ORGANIZATIONS
ASSESSMENT GUIDE

INTRODUCTION

This document provides a suggested approach for completing the Recipient Control Environment Assessment Checklist, as well as guidelines for using the results.

PERFORMING THE EVALUATION

Many of the elements addressed in the checklist may be evaluated as a part of pre-award surveys, desk reviews, or site visits.

PRE-AWARD SURVEY: Site visits by M/MPI and M/OP indicated that a number of Mission Controller offices are already using a pre-award survey that is very similar to the risk assessment checklist. Applicable components of the checklist should be addressed at this stage.

DESK REVIEWS: Most local recipients receive USAID funds on a reimbursable or periodic advance basis. Missions typically perform desk reviews of such requests, and, on occasion, verify actual costs for which the recipient is claiming to the recipient's books and records. These reviews provide not only a basis for reimbursing the recipient, but also provide valuable information about the control environment and risk assessment. For example, Risk Assessment Checklist, Part II, Approval, 4, states "Key records are matched before a transaction is approved (matching purchase order, receiving report, and vendor invoice before the invoice is approved for payment)." Requests for reimbursement or periodic advances which are not adequately supported are documented as an increased risk.

SITE VISITS: Visits to local recipients by qualified Mission financial personnel to complete the checklist are an integral part of the program. However, site visits by

Activity Managers or other SO team members can also provide valuable information. For example, Risk Assessment Checklist, Part V, Safeguards Over Access To And Use Of Assets And Records, 4, states "Assets and records are protected against physical harm." Part VI, Independent Checks, 5, states "Management reviews performance reports." Non-financial Mission personnel can determine whether these types of controls exist and can help the Controller's office maintain an up-to-date status on the recipient's control environment.

ELEMENTS OF THE CHECKLIST

The elements of the checklist are phrased so as to elicit a yes/no answer. Not applicable (N/A) is also a valid answer. For example, one control environment element states, "There is high turnover of management personnel". The Mission may not be familiar enough with the new recipient to determine whether the organization encountered high turnover of management personnel. Therefore, that element would be identified as N/A. As the organization matures and a history is developed, the response should be changed to yes or no. Each response, yes, no, or N/A, needs to be assessed individually and collectively. Individually, so as to provide a recommended course of action for material weaknesses. Collectively, so as to place individual weaknesses in perspective and to provide an overall assessment as it relates to the adequacy of the recipient's financial management and accounting system.

The control environment sets the tone of the organization, influencing the control consciousness of its people. An understanding of the control environment serves as the framework for evaluating the overall internal controls of the organization. While much of the evaluation of the control environment is based on observation of the organization and its workings; to the extent possible, the control environment should be completed and referenced to the objective data reviewed.

DOCUMENTING THE REVIEW

The assessment checklist is the objective basis from which you will be determining the degree of oversight necessary to demonstrate proper accountability of funds provided to recipients. Proper documentation of the yes, no, and N/A responses is critical. As noted above, much of the risk

assessment will be based on your pre-award surveys and interim reviews. The risk assessment should reference the workpaper(s) in the respective files which support the yes, no, or N/A. This is where the documentation should reside. The yes, no, N/A, and reference notations should be made in the right hand column of the checklist across from the specific element being evaluated.

USING THE RESULTS

In all likelihood, Missions have been informally collecting historical information concerning local recipients' financial management systems. Some of this information has been kept as cuff records , while some is in the form of Mission "institutional knowledge". Much of the information has been from prior audits and reviews of organizations such as:

- Past findings (material or immaterial),
- Timeliness of the actions taken to correct all recommendations, and
- Adequate tracking and timely final action on all audit recommendations.

In the past, such information has served as the basis for Mission requests for recipient audits or the determination to perform detailed reviews of expenditure documentation. The use of the checklist will now assist the Mission in formally documenting this information and developing a risk level for each recipient. Based on the risk level and the results of prior reviews and audits, the following, or comparable, actions should be considered:

Overall Risk Level	Suggested Actions
High	A full scope annual recipient audit until the risk is reduced
Medium	A full scope recipient audit on 30 percent of this category every three years and interim reviews as deemed necessary

| Low | Interim reviews as deemed necessary |

Based on the percentage of "no" answers to the checklist questions, a "suggested" determination of risk level would be as follows:

High	70 percent to 100 percent of answers are NO
Medium	31 percent to 69 percent of answers are NO
Low	0 percent to 30 percent of answers are NO

It is important for Missions to recognize that local conditions, the recipient's familiarity with USAID requirements, and the type of program will all impact the determination of the risk level. As such, the above percentages should be used only as a guideline and adjusted by each Mission as appropriate.

Due to the increase of the audit requirement threshold to $300,000, Missions now have the sole oversight responsibility for recipients expending less than the threshold amount. With the limited amount of resources (personnel and dollars) available for such oversight, Missions are strongly encouraged to create and maintain a documented and supported plan for accountability of those funds. The Recipient Control Environment Assessment Checklist, used with the above or similar approach, should greatly assist the Missions in demonstrating that accountability.

591sab_121701_cd26