



**OFFICE OF INSPECTOR GENERAL**  
U.S. Agency for International Development

# USAID Lacked Key Internal Controls Over Its Models for Posting Financial Transactions

**AUDIT REPORT A-000-18-004-P**  
**NOVEMBER 2, 2017**

1300 Pennsylvania Avenue NW • Washington, DC 20523  
[oig.usaid.gov](http://oig.usaid.gov) • 202-712-1150

The Office of Inspector General provides independent oversight that promotes the efficiency, effectiveness, and integrity of foreign assistance provided through the entities under its jurisdiction: the U.S. Agency for International Development, U.S. African Development Foundation, Inter-American Foundation, Millennium Challenge Corporation, and Overseas Private Investment Corporation.

## **Report waste, fraud, and abuse**

### **USAID OIG Hotline**

Email: [ighotline@usaid.gov](mailto:ighotline@usaid.gov)

Complaint form: <https://oig.usaid.gov/content/oig-hotline>

Phone: 202-712-1023 or 800-230-6539

Mail: USAID OIG Hotline, P.O. Box 657, Washington, DC 20044-0657



## MEMORANDUM

DATE: November 2, 2017

TO: M/CFO Chief Financial Officer, Reginald W. Mitchell

FROM: IG/A/ITA Director, Mark S. Norman /s/

SUBJECT: USAID Lacked Key Internal Controls Over Its Models for Posting Financial Transactions (A-000-18-004-P)

This memorandum transmits the final report on the subject audit. Our audit objective was to determine whether USAID's Office of the Chief Financial Officer implemented key internal controls over general ledger posting models in the Phoenix Financial System to mitigate the risk of unauthorized and undocumented changes. In finalizing the report, we considered your comments on the draft and included them in their entirety in appendix B.

The report contains two recommendations. After reviewing information you provided in response to the draft report, we consider recommendations 1 and 2 resolved but open pending completion of planned activities.

We appreciate the assistance you and your staff extended to us during this audit.

# CONTENTS

INTRODUCTION.....	1
SUMMARY.....	1
BACKGROUND.....	2
KEY CONTROLS FOR GENERAL LEDGER POSTING MODELS WERE LACKING BECAUSE THEY DID NOT STEM FROM A RISK ASSESSMENT .....	3
CFO Officials Did Not Conduct a Risk Assessment.....	3
Procedures for Posting Models Were Incomplete .....	4
Controls To Separate Duties for Posting Transactions Were Inadequate.....	5
Logs Were Not Enabled To Track Posting Model Changes .....	6
CONCLUSION.....	6
RECOMMENDATIONS.....	6
OIG RESPONSE TO AGENCY COMMENTS.....	8
APPENDIX A. SCOPE AND METHODOLOGY.....	9
APPENDIX B. AGENCY COMMENTS.....	11
APPENDIX C. MAJOR CONTRIBUTORS TO THIS REPORT.....	13

---

## INTRODUCTION

Like other executive branch agencies, USAID must prepare annual statements summarizing its financial activities and status at yearend to show the public how well it has managed its funds.<sup>1</sup> To produce its statements, USAID relies on the financial management system it uses to automate day-to-day accounting entries, Phoenix. In that system, electronic models are used to record or post transactions to the general ledger, which is the master set of accounts that summarizes all transactions occurring within an entity. Posting models determine which general ledger accounts are affected by each accounting transaction. Since transactions can be worth billions of dollars, and annual totals processed by Phoenix exceed \$15 billion, USAID must take care to post the transactions correctly to ensure accurate financial statements.<sup>2</sup>

The Office of Inspector General (OIG) conducted this audit in support of financial statement audits, which in fiscal years 2015 and 2014 revealed differences between USAID's general and subsidiary ledgers.<sup>3</sup> These errors occurred because USAID did not have adequate internal controls to prevent and detect errors when posting to the general ledger. Therefore, we conducted this audit to determine whether USAID's Office of the Chief Financial Officer (CFO) implemented key internal controls over general ledger posting models in Phoenix to mitigate the risk of unauthorized and undocumented changes. We defined key internal controls as policies and procedures, access controls, configuration management, and monitoring.

To conduct our work, we reviewed USAID's general ledger policies and procedures for proposing, approving, making, and documenting changes and for monitoring the posting models. We also met with CFO officials responsible for preparing USAID's annual financial statements and ensuring that USAID complies with applicable accounting standards and other Federal Government guidance. Appendix A presents our full scope and methodology.

---

## SUMMARY

Because its staff did not perform a formal risk assessment, CFO did not implement some key internal controls over the general ledger posting models in Phoenix to prevent unauthorized and undocumented changes. For example, USAID/Washington did not have clearly documented procedures for managing the general ledger posting models, nor did it have adequate security controls for tasks related to changing the models—segregating duties, maintaining audit logs (documentation), approving changes,

---

<sup>1</sup> The requirement stems from the S. 2170 — 103rd Congress: Government Management Reform Act (GMRA) of 1994.

<sup>2</sup> Annual totals come from USAID's "System Security Plan for Phoenix Financial System," May 19, 2016.

<sup>3</sup> "Control Deficiencies Identified During the Office of Inspector General's Audit of USAID's Financial Statements for Fiscal Years 2015 and 2014," February 1, 2016.

and monitoring their implementation.<sup>4</sup> As a result, USAID is at risk of having errors in the models and, thus, in its financial statements.

We are making two recommendations to help USAID improve internal controls over its general ledger posting models.

---

## BACKGROUND

The U.S. Department of the Treasury provides guidance—the U.S. Standard General Ledger<sup>5</sup>—to standardize accounting throughout the U.S. Government. The guidance includes a uniform chart of accounts, account descriptions, and technical guidance for posting transactions. Agencies set up a chart of accounts and posting models in their particular financial management systems and update the models as needed to comply with revisions to accounting standards and other Federal Government guidance.

The following provide guidance on implementing key internal controls over general ledger posting models:

- The National Institute of Standards and Technology’s (NIST) Special Publication 800-53, Rev. 4. The document states: “NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems.”
- Best practices in the U.S. Government Accountability Office’s (GAO) Federal Information System Controls Audit Manual (FISCAM).<sup>6</sup> This manual focuses on evaluating the effectiveness of internal controls for information systems, including general and application controls.
- The Office of Management and Budget (OMB) Circular A-123, “Management’s Responsibility for Internal Control.” This circular defines management’s responsibility for internal control in Federal agencies.<sup>7</sup>
- Public Law 104–208, “Federal Financial Management Improvement Act of 1996” (FFMIA). This law requires annual financial statement audits and aims to provide consistency in accounting by an agency from one fiscal year to the next, and uniform accounting standards throughout the Federal Government.

---

<sup>4</sup> Adequate security is defined in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations,” as security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information.

<sup>5</sup> Treasury Financial Manual, Section III, “U.S. Government Standard General Ledger Account Transactions.”

<sup>6</sup> GAO-09-232G, February 2009.

<sup>7</sup> OMB updated Circular A-123 in memo M-16-17 on July 15, 2016. The update added requirements. Since this update was issued during fieldwork, the auditors relied on the internal control requirements in the December 2004 version.

- Public Law 97-255, “Federal Managers’ Financial Integrity Act of 1982” (FMFIA). This law requires an annual Statement of Assurance on whether the agency has met internal control requirements such as effectiveness and efficiency of operations and reliability of financial reporting.

---

## **KEY CONTROLS FOR GENERAL LEDGER POSTING MODELS WERE LACKING BECAUSE THEY DID NOT STEM FROM A RISK ASSESSMENT**

Because it did not perform a formal risk assessment to find out where controls were most needed, USAID did not implement adequate key internal controls over general ledger posting models to mitigate the risk of unauthorized and undocumented changes. The general ledger posting model procedures omitted important details, controls to separate duties were inadequate, and monitoring and audit logs were not enabled to track posting model changes.

### **CFO OFFICIALS DID NOT CONDUCT A RISK ASSESSMENT**

OMB Circular A-123 states:

Federal managers must carefully consider the appropriate balance between controls and risk in their programs and operations. Managers should define the control environment (e.g., programs, operations, or financial reporting) and then perform risk assessments to identify the most significant areas within that environment in which to place or enhance internal control. The risk assessment is a critical step in the process to determine the extent of controls. Once significant areas have been identified, control activities should be implemented.

Contrary to the circular and the requirement to clearly document significant events,<sup>8</sup> USAID did not perform a formal written risk assessment. Therefore, USAID staff could not demonstrate that they identified which internal controls were needed to ensure accurate and complete transaction posting. CFO staff did not conduct a formal written risk assessment because they said the consideration of risk is an inherent part of preparing procedures for posting financial transactions.

---

<sup>8</sup> GAO’s “Standards for Internal Control in the Federal Government,” section 10.03, “Design of Appropriate Types of Control Activities,” September 2014.

## **PROCEDURES FOR POSTING MODELS WERE INCOMPLETE**

As a best practice, FISCAM encourages agencies to develop policies and procedures for maintaining data.<sup>9</sup> Written procedures should specify data quality criteria, approval requirements, and supporting documents for changes to data that affect the general ledger,<sup>10</sup> including the general ledger posting models that generate the data. FISCAM also states that the data maintenance process should include a “formal create/change request from the requestor and approval from the data owner.”

However, the “General Ledger (GL) Posting Model Procedures” that CFO issued on September 30, 2015, in response to a finding by the fiscal year 2015/2014 financial statement auditors does not:

- Specify who is responsible for identifying and recommending changes to the general ledger posting models.
- Describe how to request a change, including a description of what is considered a valid or justified change.
- Specify a record-keeping process for recommended changes.
- Address documentation of approved changes to general ledger posting models before they are put into effect.
- Detail each step in the process. For example, one procedure states, “[A]ny changes that are applicable and necessary are identified and recommended to [the general ledger] Team Lead or ... [CFO division] Chief for . . . approval.” However, it was not clear what the general ledger team leader or chief should review before granting approval.
- Require the data owner to formally approve and document approval for changes to the posting models.

Inadequate procedures present the following risks:

- If procedures do not contain adequate controls, changes to the general ledger may be made without proper review and approval, increasing the risk of errors and making it more difficult for USAID to comply with FFMI, which requires Federal financial managers to ensure that their systems provide accurate and reliable financial management information.
- If procedures are unclear or incomplete, staff—especially new employees—may not be able to apply them or keep the posting models up-to-date, resulting in delays and risks to the integrity of the financial data.

---

<sup>9</sup> Section BP-4.4.1.

<sup>10</sup> These data are known as master data, which FISCAM defines as information that “provides the basis for ongoing business activities such as the organizational structure, general ledger account structure, and vendor or employee information.”

- Further, because the procedures did not require the data owner to formally approve and document changes before the changes were implemented, the Agency heightened the risk of errors to the data, since not approving changes may increase the need for adjusting entries and overriding error codes.

## **CONTROLS TO SEPARATE DUTIES FOR POSTING TRANSACTIONS WERE INADEQUATE**

To reduce the risk of abuse of authorized privileges, NIST and FISCAM state that organizations need to separate employees' duties, document the separated duties, and limit information system access so that it reflects that separation.<sup>11</sup> Segregation of duties involves more staff in a process to reduce the risk that errors could be undetected.

However, USAID did not have adequate segregation of duties for proposing, approving, making, and reviewing changes to the general ledger posting models. Specifically, the general ledger team leader could perform all steps in the process as presented in the CFO's "General Ledger (GL) Posting Model Procedures."

A contributing factor to the lack of segregation was that USAID's "Washington Phoenix User Roles as of 9/14/15" did not identify conflicting roles for the general ledger table administrator. The table administrator was the only one who could make changes to the posting models. The general ledger team leader and another team member held both the general ledger table administrator and general ledger accounting supervisor roles in Phoenix. By also holding the general ledger accounting supervisor role, they could also process vouchers to (1) adjust the general ledger, (2) reclassify expenditures, and (3) cancel uncollectable debts. Thus, an individual with both the table administrator and supervisor roles could theoretically post transactions and also change the accounts they are posted to, increasing the risk of undetected errors and manipulation.

Even without intentional wrongdoing, this lack of segregation increased the risk of undetected errors. In making changes to posting models, the general ledger table administrators were permitted to override error codes, one of which states: "Changing the account classification may cause existing general ledger account entries to no longer be self-balancing [i.e., accurate]." USAID records showed that one user had overridden that code 49 times, 126 times, and 106 times during fiscal years 2014, 2015, and 2016, respectively; another user had overridden it 6 times in fiscal year 2016.<sup>12</sup>

USAID officials said they have no log of what errors may have been caused by overriding the warning. They said that if a change to a general ledger account was made incorrectly, the mistake would become apparent later, for example during the reconciliation between the general ledger and the subsidiary ledger.

---

<sup>11</sup> NIST SP 800-53 (Revision 4), Control AC-5 Separation of Duties; Federal Information System Controls Audit Manual (FISCAM), GAO-09-232G, February 2009.

<sup>12</sup> We reviewed override records for fiscal years 2014, 2015, and 2016.

If the CFO does not allocate resources to implement adequate segregation of duties, it must implement compensating controls to mitigate the associated risks. Such controls include periodic independent reviews, system activity logs, or automated records of posting model changes.

## **LOGS WERE NOT ENABLED TO TRACK POSTING MODEL CHANGES**

When duties are not segregated, FISCAM advocates that agencies implement compensating controls.<sup>13</sup> Among the controls that meet NIST requirements are records to categorize events (entries or transactions); tell when, where, and why they occurred; document their outcome; and identify any individuals associated with them.<sup>14</sup>

USAID did not turn on the Phoenix logs to track general ledger posting model changes or who made them. Moreover, even if CFO had turned on the logs, it lacked a formal process for monitoring the logs or other documentation of changes. Even though the general ledger team leader began using a manual verification log in fiscal year 2016, he was documenting and reviewing his own work. By not monitoring general ledger posting models and user activity, the Agency increases the risk of not detecting and correcting errors.

---

## **CONCLUSION**

OMB guidance calls for Federal managers to carefully consider the relevant risks and implement internal controls in all of their programs and operations. While CFO staff said that they consider risks while they are preparing procedures, they lacked a thorough and documented assessment of the risks associated with the general ledger posting models. Until USAID considers all the risks and implements adequate internal controls as outlined in this report, it lacks reasonable assurance that it is preventing and detecting errors in the general ledger posting models, complicating its ability to comply with applicable Federal requirements.

---

## **RECOMMENDATIONS**

We recommend that USAID's chief financial officer take the following actions:

- I. Perform a written risk assessment of its general ledger posting model process, as required by Office of Management and Budget Circular A-123. The risk assessment

---

<sup>13</sup> FISCAM Application Security (AS) control, AS-4, "Segregate user access to conflicting transactions and activities and monitor segregation," February 2009.

<sup>14</sup> NIST SP 800-53, Control AU-3, "Content of Audit Records," April 2013.

should include cost-benefit considerations and a plan to implement compensating or appropriate internal controls to prevent and detect errors. The risk assessment should address:

- Segregation of duties.
- Data owner approval of changes to the general ledger posting models.
- Records of all steps in procedures.
- Use of activity or transaction logs for monitoring.

The risk assessment should also document the acceptance of all risks that will not be mitigated.

2. Update and implement USAID's general ledger posting model procedures, after taking final corrective action on recommendation I, to include explicit roles and responsibilities and a step-by-step process for updating the posting models.

---

## **OIG RESPONSE TO AGENCY COMMENTS**

We provided USAID officials with our draft report on September 7, 2017, and on October 6, 2017, we received management's response, which is included in appendix B. The Agency accepted both of our recommendations and provided corrective action plans, including target completion dates. We acknowledge the Agency's management decisions on both recommendations and consider both of them resolved but open pending completion of planned activities.

---

## APPENDIX A. SCOPE AND METHODOLOGY

The audit scope covered the Office of the Chief Financial Officer's controls over the general ledger posting models in Phoenix. We conducted our work at USAID's headquarters in Washington, DC, from March 25, 2016, through September 7, 2017, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

We reviewed USAID's policies and procedures for its general ledger posting models to determine whether there were requirements and internal controls for approving changes to the models, monitoring those changes, and documenting those activities.

We interviewed CFO officials in Washington, DC, including the chief financial officer, deputy chief financial officer, and staff in the Central Accounting and Reporting Division and Financial Systems Divisions. We also interviewed staff from the Office of the Chief Information Officer. We assessed access controls for all of USAID's system administrators with permissions to change general ledger posting models. We evaluated the appropriateness of the number of those administrators and whether any other staff or departed administrators still had access to change the posting models in Phoenix.

The computer-processed data used in this report were independently extracted by an OIG information technology specialist. To assess the reliability of Phoenix user access roles and the data on overriding error codes, we reviewed his methodology and inquired about the accuracy of the data. The specialist compared information retrieved from existing Phoenix reports with information he pulled directly from the Phoenix database and concluded that creating specific queries tailored to the audit team's needs provided more accurate information than relying on the existing Phoenix reports. Also, we discussed the information with USAID officials. We determined that the data were sufficiently reliable for the purposes of this report.

We reviewed USAID's "Application Operation and Maintenance Configuration Management Plan" to determine if requirements were applicable to general ledger posting model changes and, if applicable, whether the staff were in compliance. We reviewed the process for monitoring general ledger posting models. Also, we verified whether audit and transaction logs were enabled, maintained, and reviewed in Phoenix for fiscal year 2016.

We assessed the aforementioned controls using the following criteria:

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013.

- Public Law 104–208, “Federal Financial Management Improvement Act of 1996” (FFMIA), September 1996.
- Office of Management and Budget (OMB), M-13-23, Appendix D to Circular A-123, “Compliance with the Federal Financial Management Improvement Act of 1996,” September 2013.
- Public Law 97-255, “Federal Managers’ Financial Integrity Act of 1982,” September 1982.
- Office of Management and Budget, OMB Circular A-123, “Management’s Responsibility for Internal Control,” December 2004.<sup>15</sup>
- U.S. Government Accountability Office, FISCAM, GAO-09-232G, February 2009.

---

<sup>15</sup> OMB updated Circular A-123 in memo M-16-17 on July 15, 2016. This update added requirements for agencies to implement Enterprise Risk Management capabilities. Since this update was issued during fieldwork, the auditors relied on the internal control requirements in the December 2004 version.



**USAID**  
FROM THE AMERICAN PEOPLE

---

## APPENDIX B. AGENCY COMMENTS

*Chief Financial Officer*

September 22, 2017

### MEMORANDUM

**TO:** Tom Yatsco, Assistant Inspector General for Audit

**FROM:** Reginald W. Mitchell /s/

**SUBJECT:** Management Response to Draft Report on USAID's Model for Posting Financial Transactions Lacked Key Internal Controls (A-000-17-00X-P)

Thank you for the opportunity to respond to the draft audit report. The Office of the Chief Financial Officer has reached a management decision for the following two recommendations:

**Recommendation I:** We recommend that USAID's Chief Financial Officer perform a written risk assessment of its general ledger posting model process, as required by Office of Management and Budget Circular A-123. The risk assessment should include cost-benefit considerations and a plan to implement compensating or appropriate internal controls to prevent and detect errors. The risk assessment should address:

- Segregation of duties.
- Data owner approval of changes to the general ledger posting models.
- Records of all steps in procedures.
- Use of activity or transaction logs for monitoring.

The risk assessment should also document the acceptance of all risks that will not be mitigated.

**Management Decision:** USAID management accepts this recommendation and will conduct a written risk assessment of its general ledger posting model maintenance procedures. USAID management believes that the risks identified by the OIG have been mitigated in M/CFO/CAR's procedure updates during FY 2017 and that the risk assessment will provide the OIG these assurances.

**Target Completion Date:** January 31, 2018.

**Recommendation 2:** We recommend that USAID’s Chief Financial Officer update and implement USAID’s general ledger posting model procedures, after taking final corrective action on recommendation 1, to include explicit roles and responsibilities and a step-by-step process for updating the posting models.

**Management Decision:** USAID management accepts this recommendation and will take corrective action if the risk assessment identifies areas for improvement in M/CFO/CAR’s posting model maintenance procedures.

**Target Completion Date:** April 30, 2018.

---

## **APPENDIX C. MAJOR CONTRIBUTORS TO THIS REPORT**

The following made major contributions to this report: Mark Norman, director, Information Technology Audits Division; Lisa Banks, assistant director, Information Technology Audits Division; Eunice Valentin Rivera, information technology auditor; Tiara Jackson, information technology auditor; Richard Puerto, information technology specialist; George D'Elia, information technology specialist; and Lisa McCabe, program analyst.