



U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

**AUDIT REPORT
15-03**

**U.S. Government Publishing Office FY 2014
Independent Auditor's Report**

February 5, 2015



Date

February 5, 2015

To

Director, U.S. Government Publishing Office

From

Inspector General

Subject:

FY 2014 Independent Auditor's Report
Report Number 15-03

Attached is the Independent Auditor's Report on the U.S. Government Publishing Office's (GPO's) FY 2014 financial statements. We contracted with the independent certified public accounting firm of KPMG LLP (KPMG) to audit the financial statements of GPO as of and for the years ending September 30, 2014, and 2013. The contract required that the audit be conducted in accordance with generally accepted government auditing standards (GAGAS).

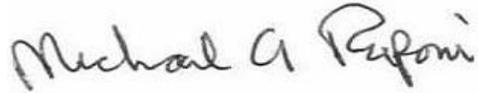
KPMG's opinion on GPO's financial statements was unqualified. KPMG's consideration of internal control resulted in one significant deficiency related to controls over financial reporting and one significant deficiency related to Information Technology General and Application Controls. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

The significant deficiency in controls over financial reporting is an improvement from the FY 2013 audit at which time the deficiency was reported as a material weakness. KPMG made recommendations that GPO address each of the deficiencies.

KPMG is responsible for the attached auditor's report and the conclusions expressed in the report. However, in connection with the contract, we reviewed KPMG's report and related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with GAGAS, was not intended to enable us to express, and we do not express, an opinion on GPO's financial statements; or conclusions about the effectiveness of any internal control; or on GPO's compliance with laws and regulations. Our review did not disclose any

instances where KPMG did not comply, in all material respects, with GAGAS requirements.

We appreciate the courtesies extended to KPMG and to our audit staff. If you have any questions or comments about this report, please do not hesitate to contact me at (202) 512-0039.

A handwritten signature in black ink that reads "Michael A. Raponi". The signature is written in a cursive, slightly slanted style.

MICHAEL A. RAPONI
Inspector General

Attachment

cc:

Deputy Director, U.S. Government Publishing Office
General Counsel
Chief of Staff
Chief Financial Officer



KPMG LLP
Suite 12000
1801 K Street, NW
Washington, DC 20006

Independent Auditors' Report

Director
United States Government Publishing Office

Office of the Inspector General
United States Government Publishing Office:

Report on the Financial Statements

We have audited the accompanying consolidated financial statements of the United States Government Printing Office (GPO), which comprise the consolidated balance sheets as of September 30, 2014 and 2013, and the related consolidated statements of revenues, expenses, and changes in retained earnings, and cash flows for the years then ended, and the related notes to the consolidated financial statements.

Management's Responsibility for the Financial Statements

Management is responsible for the preparation and fair presentation of these consolidated financial statements in accordance with U.S. generally accepted accounting principles; this includes the design, implementation, and maintenance of internal control relevant to the preparation and fair presentation of consolidated financial statements that are free from material misstatement, whether due to fraud or error.

Auditors' Responsibility

Our responsibility is to express an opinion on these consolidated financial statements based on our audits. We conducted our audits in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards*, issued by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain reasonable assurance about whether the consolidated financial statements are free from material misstatement.

An audit involves performing procedures to obtain audit evidence about the amounts and disclosures in the consolidated financial statements. The procedures selected depend on the auditors' judgment, including the assessment of the risks of material misstatement of the consolidated financial statements, whether due to fraud or error. In making those risk assessments, the auditor considers internal control relevant to the entity's preparation and fair presentation of the consolidated financial statements in order to design audit procedures that are appropriate in the circumstances, but not for the purpose of expressing an opinion on the effectiveness of the entity's internal control. Accordingly, we express no such opinion. An audit also includes evaluating the appropriateness of accounting policies used and the reasonableness of significant accounting estimates made by management, as well as evaluating the overall presentation of the consolidated financial statements.

KPMG LLP is a Delaware limited liability partnership,
the U.S. member firm of KPMG International Cooperative
("KPMG International"), a Swiss entity.



We believe that the audit evidence we have obtained is sufficient and appropriate to provide a basis for our audit opinion.

Opinion on the Financial Statements

In our opinion, the consolidated financial statements referred to above present fairly, in all material respects, the financial position of the United States Government Printing Office as of September 30, 2014 and 2013, and the results of its operations and its cash flows for the years then ended in accordance with U.S. generally accepted accounting principles.

Other Matters

Other Information

Our audits were conducted for the purpose of forming an opinion on the basic consolidated financial statements as a whole. The information in the Management's Discussion and Analysis section is presented for purposes of additional analysis and is not a required part of the basic consolidated financial statements. Such information has not been subjected to the auditing procedures applied in the audits of the basic consolidated financial statements, and accordingly, we do not express an opinion or provide any assurance on it.

Other Reporting Required by Government Auditing Standards

Internal Control over Financial Reporting

In planning and performing our audit of the consolidated financial statements as of and for the year ended September 30, 2014, we considered GPO's internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of GPO's internal control. Accordingly, we do not express an opinion on the effectiveness of GPO's internal control.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses. However, we did identify certain deficiencies in internal control, described in the accompanying Schedule of Findings as items 2014-01 and 2014-02, which we consider to be significant deficiencies.



Compliance and Other Matters

As part of obtaining reasonable assurance about whether the GPO's consolidated financial statements are free from material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, and contracts, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests of compliance disclosed no instances of noncompliance or other matters that are required to be reported herein under *Government Auditing Standards*.

GPO's Responses to Findings

The GPO's responses to the findings identified in our audit are described in the accompanying Schedule of Findings. The GPO's responses were not subjected to the auditing procedures applied in the audit of the consolidated financial statements and, accordingly, we express no opinion on the responses.

Purpose of the Other Reporting Required by Government Auditing Standards

The purpose of the communication described in the Other Reporting Required by *Government Auditing Standards* section is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the GPO's internal control or compliance. Accordingly, this communication is not suitable for any other purpose.

KPMG LLP

February 2, 2015

Schedule of Findings

Fiscal Year 2014 Significant Deficiencies

2014-01 Controls over Financial Reporting

In Fiscal Year (FY) 2013, we noted several matters that highlighted the need for improved controls over financial reporting in several key process areas. Although the Office of the Chief Financial Officer implemented policies and procedures in FY 2014 that improved controls over financial reporting, we noted that certain monthly account balance reconciliations and activities performed by accounting and finance staff were not timely prepared and reviewed by a supervisor. We also noted several instances where supervisory reviews were not adequately performed to detect errors in the reconciliations and account activities. Collectively, these matters are considered to be a significant deficiency in internal control over financial reporting. Specifically, we noted the following:

- The billings to revenue reconciliations for March and June 2014 were prepared using an incorrect FY 2014 beginning balance that did not agree to the amounts in the FY 2013 audited financial statements.
- The Government accounts receivable balance reported in the FY 2014 “4 Bucket Report”, used by GPO to calculate the allowance for doubtful accounts as of September 30, 2014, exceeded the Government accounts receivable balance reported in the general ledger by \$5.6 million. This difference was not investigated by GPO staff. Upon our review of the “4 Bucket Report,” we noted that the report included items, such as Intra-governmental Payment and Collection (IPAC) chargebacks and commercial accounts receivable that should have been excluded. This resulted in an overstatement of the allowance for doubtful accounts by \$948,452 as of September 30, 2014.
- The lag factor schedule used to estimate procured printing year end accrued expenses contained multiple mathematical errors which resulted in the overstatement of the accrual and expenses by approximately \$891,356, and revenue by approximately \$953,750, for the year ended September 30, 2014. We also noted that the lag factor accrual schedule did not take into account the last three months of the year resulting in an understatement of the accrual and expenses by approximately \$1,576,424, and an understatement of revenue by approximately \$1,686,744, for the year ended September 30, 2014.
- The March 2014 general ledger closed on May 9, 2014, however, we noted that several reconciliations were not performed and reviewed until June. For example, the March 2014 Work In process (WIP) reconciliation was prepared on June 10th and reviewed on June 17th and the March 2014 salaries payable and accrued annual leave reconciliations were prepared on June 11th and reviewed on June 16th.
- During our testwork over advanced billing, we noted that one out of three transactions tested in the amount of \$60,248 was incorrectly recorded as advanced billing. The project related to this transaction was completed and final billed in July 2014. Accordingly, this amount should have been recognized as revenue in FY 2014.
- During our testwork over unbilled accounts receivable, we tested a sample of 7 transactions and noted that unbilled accounts receivable and revenue, as of and for the year ended September 30, 2014, were overstated by approximately \$67,979, as a result of the following:
 - The related project for one of the transactions was completed during July 2014 and no further billings were anticipated. However, there is a remaining unbilled accounts receivable balance of \$43,356 as of September 30, 2014 which should have been reversed by charging it to the billing variance account.

- Unbilled accounts receivable and revenue were overstated by the amount of \$24,623 that relates to an unapplied materials credit that was not timely recorded prior to September 30, 2014.

The above issues occurred due to a lack of adequate supervisory review of the reconciliations and the detail of account balances and related activities. In addition, GPO's policies and procedures do not include specific guidance on the review procedures of the account reconciliations and activities that would guide GPO supervisors during their reviews.

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* states:

"Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements or budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.

Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as 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 as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes."

Management reviews are considered a key aspect of control monitoring. Examples of control activities include reviews by management at the functional or activity level. Specifically, the *Standards for Internal Control in the Federal Government* states:

"Internal control should generally be designed to assure that ongoing monitoring occurs in the course of normal operations. It is performed continually and is ingrained in the agency's operations. It includes regular management and supervisory activities, comparisons, reconciliations, and other actions people take in performing their duties."

Financial Procedure 0004 General Ledger Account Reconciliations states:

"The Director, Accounting Operations shall determine reconciliations assignments, which are normally due 5 business days after every monthly close except September."

Recommendations:

We recommend that GPO management:

1. Continue to improve the controls in place over the preparation and review of periodic reconciliations to ensure that the reconciliations are adequately prepared and reviewed in a timely manner.
2. Develop and implement more detailed policies and procedures to guide supervisors during their review of the various accounts balances and related activities to ensure that the consolidated financial statements are properly stated at fiscal year end.

Management Response:

Management concurs with the finding. GPO management will continue to monitor the reconciliations for timeliness and accuracy during fiscal year 2015 as well as continue the CFO-led reconciliation review meetings to work on identified weaknesses. We will develop a more efficient aging report to review the allowance for doubtful accounts with a draft completed by June 30, 2015. The reconciliation review meetings will begin in February ending after all the account reconciliations have been reviewed satisfactorily and the monitoring of the reconciliations will continue through the fiscal year. In addition, the Office of the Plant Controller has a procedure in effect to review quarterly all plant monthly projects and plant projects more than three years old. This review procedure will be expanded to include all plant jackets. The next quarterly review will take place in February 2015. In projects where no further billings are anticipated and a variance has yet to be recognized, a negative billing variance will be recognized for any revenue remaining in unbilled accounts receivable. Accounting Operations will develop a finance procedure for adding revenue from invoices to projects (to include correcting errors).

2014-02 Internal Controls over Information Technology General and Application Controls

During FY 2014, we identified deficiencies in the design and/or operations of GPO's information technology (IT) general controls in the areas of Security Management, Access Controls, Segregation of Duties, and Contingency Planning. These deficiencies were generally due to resource constraints and competing priorities at GPO. The details of these conditions, several of which have been reported to management in prior years' audit reports, are as follows:

Security Management

Security management is the foundation of a security control structure that includes a framework to document security plans and procedures. GPO's major application - Procurement Information Control System (PICS) - did not have a finalized Certification and Accreditation (C&A) package. GPO's IT Security function does not have the resources to perform a security certification review of PICS. Accordingly, GPO started the process and plans to have it completed in FY 2015.

The lack of completed C&A package documentation means that system security risks and requirements have not been documented and assessed, increasing the likelihood of unidentified threats compromising the integrity and confidentiality of GPO financial information.

GPO Directive 825.33B: *Information Technology (IT) Security Program Statement of Policy*, dated May 2011, states:

“The Certification is the evaluation of IT system(s) security controls to ensure they are implemented and to determine the residual risk. Accreditation is the acceptance by the Designed Approving Authority (DAA) of the residual risk by senior management, based on threats to the system and the implemented security controls (the DAA may grant interim authority to operate on a case by case basis.) Systems will undergo C&A before they process any data. Additionally, systems will be re-accredited at least every 3 years, or when a significant change is made to the configuration of the system.”

Access Controls

Overall, access controls at GPO continue to require strengthening in order to provide a more secure financial processing and computing environment. GPO management made progress in addressing the access control deficiencies noted in prior years. However, we noted the following access control deficiencies that need improvement:

- The General Support System's (GSS) Active Directory (AD) is not configured to disable inactive user workstations. Instead, session timeout is configured at the individual workstation.
- GPO does not have a process in place to perform and document a periodic review of personnel with access to the IT GSS Platform to determine whether user access is appropriate.
- During our testwork, we identified 117 former employees that separated from GPO during the current year, and we noted the following:
 - 28 separated employees retained active GPO's Oracle Financials (GBIS) accounts for a period ranging from 31 to 114 days after their separation date. In addition, 2 of the 28 users attempted to login after their separation date.
 - 66 separated employees retained an active GSS account for a period ranging from 36 to 336 days after their separation date. In addition, 2 of the 66 users attempted to login after their separation date.
 - One separated employee retained an active PICS account for 84 days after their separation date.

GPO's current policies do not require session locks for the GSS to be configured within AD or to perform annual review of user's access. In addition, supervisors are not consistently following the account termination policies and procedures for separated users.

Failure to enforce consistent configuration settings, reviewing user access and disabling user accounts for terminated individuals increases the risk that the confidentiality and integrity of information and information systems will be compromised.

National Institute of Standard and Technology (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, Control AC-11, *Session Lock* states:

“The information system:

1. Prevents further access to the system by initiating a session lock after [*Assignment: organization-defined time period*] of inactivity or upon receiving a request from a user; and
2. Retains the session lock until the user reestablishes access using established identification and authentication procedures”

GPO Directive 825.33B states:

“User lists and privileges will be periodically reviewed. The review will be the basis for modifying access levels, including denying access to individuals as a result of task changes or changes in employment status.”

“Access control lists will be reviewed and updated on a periodic basis. Access will be denied to individuals who have been terminated or, at the discretion of management, to those that are the subject of adverse personnel actions.”

“Access will be denied to individuals who have been terminated, or at the discretion of management, to those that are the subject of adverse personnel actions.”

“Each system will have a process in place that ensures individuals are denied access to the system when employment is terminated, at the discretion of management, or are the subject of adverse personnel actions.”

Segregation of Duties

Effective segregation of duties starts with effective entity-wide policies and procedures that are implemented at the system and application levels. GPO has not implemented automated controls to enforce segregation of duties to prevent conflicting roles from being assigned to a GBIS user. GPO stated they are in the process of implementing the Oracle Governance, Risk, and Compliance (GRC) module to automate the process to enforce segregation of duties.

Without the proper alignment of the segregation of duties procedures and the system user listing it makes it difficult for management to identify and monitor users with conflicting roles and responsibilities. This increases the likelihood that users with conflicting roles and responsibilities can go undetected.

GPO Directive 825.33B states:

“Access controls will enable the use of only the resources, such as data programs, necessary to fulfill an individual's job responsibilities and will enforce separation of duties based on roles and responsibilities.”

Contingency Planning

Losing the capability to process, retrieve, and protect data can significantly impact an agency's ability to accomplish its mission. For this reason, an agency should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions, and (2) a plan to recover critical operations should interruptions occur. GPO did not finalize, approve and fully test the contingency plan for its general support system because the Office 365 project was not complete.

Without an effective contingency plan and testing process in place, GPO may not be able to successfully recover critical applications and systems to maintain business functions during the event of a service disruption.

GPO Directive 825.33B states:

“The GPO will safeguard its IT systems through the implementation of the GPO IT Security Program, which will accomplish the following: Define, document, and manage the contingency planning process, including training and testing, to provide IT systems with adequate continuity of operations upon disruption of normal operations.”

“The Chief Information Officer (CIO) is responsible for developing and maintaining an agency-wide IT Security Program, including providing for the continuity of operations in the event of system disruption. Contingency plan means a plan for emergency response, back-up operations, and post-disaster recovery for IT systems and installations in the event normal operations are interrupted. The contingency plan should ensure minimal impact upon data processing operations in the event the IT system or facility is damaged or destroyed.”

Recommendations:

We recommend that the Chief Information Officer (CIO):

Security Management

1. Complete the C&A package and supporting documents for PICS.

Access Controls

2. Update GPO's policies and procedures to require the Information Technology division to modify the GSS AD settings and include session timeout or distribute guidance to GPO personnel in order to inform them of recommended session timeout settings.
3. Formally document policies and procedures for periodically reviewing access to the GPO GSS to help ensure that access is reviewed on a defined frequency and that the review is documented and implement controls to monitor compliance for the periodic review.
4. Update GPO's policies and procedures for the timely removal of terminated users from GPO systems. This policy should also include a timeframe for removal of terminated users.
5. Communicate to supervisors the importance of timely submitting access termination request forms to system owner to allow for terminated users to be removed in a timely manner.
6. Increase the frequency that management monitors the timely removal of user access from GPO systems.

Segregation of Duties

7. Ensure that the implementation of the GRC Module for GBIS to automate segregation of duties is implemented by February 2015, the scheduled completion date.

Contingency Planning

8. Finalize and approve the contingency plan for GSS and periodically perform contingency plan testing and document the results.

Management Response:

Management concurs with all conditions noted.