U.S. GOVERNMENT PUBLISHING OFFICE

OFFICE OF INSPECTOR GENERAL

AUDIT REPORT
REPORT NUMBER 18-04

Financial Management: Internal Controls Over Financial Reporting

February 5, 2018

U.S. GOVERNMENT PUBLISHING OFFICE
OFFICE OF INSPECTOR GENERAL

Date

February 5, 2018

To

Chief Financial Officer
Acting Chief Information Officer

From

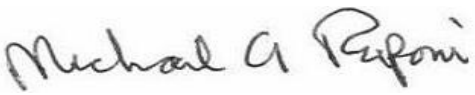
Inspector General

Subject:

Audit Report—Financial Management: Internal Controls Over Financial Reporting
Report Number 18-04

Enclosed please find the subject final report. Please refer to the "Results in Brief" for the overall audit results. Our evaluation of your response has been incorporated into the body of the report. We consider management's comments responsive to the recommendations, which are considered resolved but will remain open until implementation of the proposed corrective actions.

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



MICHAEL A. RAPONI
Inspector General

Attachment

cc:
Acting Director, GPO
Chief of Staff
Chief Administrative Officer
Acting General Counsel

Contents

Office of Inspector General

Report Number 18-04 **February 5, 2018**

Financial Management: Internal Controls Over Financial Reporting

Introduction

GPO's policy requires that it maintain an effective system of accounting and management controls. The Government Accountability Office (GAO) "Standards for Internal Control in the Federal Government" or "*Green Book*"[1], sets the standards for an effective internal control system and provides the overall framework for designing, implementing, and operating an internal control system. The *Green Book* approaches internal control through a hierarchical structure of five components and seventeen principles. The seventeen principles support the effective design, implementation, and operation of the associated components.

An analysis was performed to identify differences—gaps—between applicable *Green Book* principles and GPO's internal control framework over financial reporting. To accomplish our objective, we interviewed responsible officials, reviewed Federal regulations and laws, reviewed GPO policies and procedures, and contracted with KPMG to compare GPO's internal control framework to applicable *Green Book* principles.

Results in Brief

The analysis identified the need to strengthen key controls pertaining to the risk assessment processes and the design and implementation of control activities over financial reporting. The analysis also revealed GPO could strengthen controls over the design and implementation of control activities associated with financial information systems.

Recommendations

OIG made 14 recommendations that would help improve internal controls over financial reporting.

Management's Response

Management concurred with the recommendations. The complete text of management's response is in Appendix C.

[1] Standards for Internal Control in the Federal Government, GAO-14-704G, September 2014.

Background

GPO requires[2] that management controls provide reasonable assurance and safeguards to protect assets against waste, loss, unauthorized use, and misappropriation. The guidance states that GPO must maintain effective systems of accounting and management control. The policy also states that internal controls are the organization, policies, and procedures used to reasonably assure that resources are used consistent with agency mission and resources are protected from waste, fraud, and mismanagement.

The *Green Book* consists of five components of internal control that represent the highest level of the hierarchy of standards in the federal government. Seventeen underlying principles have been introduced to support the five overarching components of internal control. The figure below generally depicts the components and principles.

Figure 1. General Description of the Five Components and 17 Principles of Internal Control

Control Environment

1. The oversight body and management should demonstrate a commitment to integrity and ethical values.

2. The oversight body should oversee the entity's internal control system.

3. Management should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

4. Management should demonstrate a commitment to recruit, develop, and retain competent individuals.

5. Management should evaluate performance and hold individuals accountable for their internal control responsibilities.

Risk Assessment

6. Management should define objectives clearly to enable the identification of risks and define risk tolerances.

7. Management should identify, analyze, and respond to risks related to achieving the defined objectives.

8. Management should consider the potential for fraud when identifying, analyzing, and responding to risks.

9. Management should identify, analyze, and respond to significant changes that could impact the internal control system.

Control Activities

10. Management should design control activities to achieve objectives and respond to risks.

11. Management should design the entity's information system and related control activities to achieve objectives and respond to risks.

12. Management should implement control activities through policies.

Information and Communication

13. Management should use quality information to achieve the entity's objectives.

14. Management should internally communicate the necessary quality information to achieve the entity's objectives.

15. Management should externally communicate the necessary quality information to achieve the entity's objectives.

Monitoring

16. Management should establish and operate monitoring activities to monitor the internal control system and evaluate the results.

17. Management should remediate identified internal control deficiencies on a timely basis.

Source: GAO. | GAO-14-704G

The following four *Green Book* principles were determined to be in scope for the purpose of the analysis.

- Principle 7—Identify analyze, and respond to risks
- Principle 10—Design control activities
- Principle 11—Design activities for the information system
- Principle 12—Implement control

[2] GPO Instruction 825.18A, *Internal Control Program*, dated May 28, 1997.

Results and Recommendations

The assessment identified the following internal control differences—gaps. Gap numbers 1, 2, and 4 are within the Chief Financial Officer's area of responsibility. Gap number 3 is within the Chief Information Officer's area of responsibility.

***Green Book* Requirements**			**Gaps**
Principle Number	**Principle Description**	**Attribute**	
7	Identify, Analyze, and Respond to Risks	Identification of Risks	Gap 1 – Key internal controls, activities, and/or processes to address the attribute, principle and/or component are needed.
		Analysis of Risks	
		Response to Risks	
10	Design Control Activities	Response to Objectives and Risks	Gap 2 – The attribute, principle and/or component are being addressed by key internal controls, activities and/or processes performed by GPO; however improvements are needed.
		Design of Appropriate Types of Control Activities	
		Design of Control Activities at Various Levels	
		Segregation of Duties	
11	Design Activities for the Information System	Design of the Entity's Information System	Gap 3 – The attribute, principle and/or component are being addressed by key internal controls, activities and/or processes performed by GPO; however improvements are needed.
		Design of Appropriate Types of Control Activities	
		Design of Information Technology Infrastructure	
		Design of Security Management	
		Design of Information Technology Acquisition, Development, and Maintenance	
12	Implement Control Activities	Documentation of Responsibilities through Policies	Gap 4 – The attribute, principle and/or component are being addressed by key internal controls, activities and/or processes performed by GPO; however improvements are needed.
		Periodic Review of Control Activities	

Gap 1: Risk Assessment

According to GPO's *Accounting Policies Manual*, dated March 28, 2017, Section 9-5, business units must identify risks that could impede efficient and effective achievement. The business unit managers must prepare a risk assessment summary and provide general conclusions and actions needed. Each Finance unit performing a risk assessment must provide a Statement of Assurance about the effectiveness of its internal controls over financial reporting for the period ending on the review date.

As a result of activities such as continuous system upgrades and/or conflicting priorities, the risk assessment was not performed in accordance to the *Accounting Policies Manual*.

Recommendations

Recommendation 1: We recommend that the Chief Financial Officer develop and implement a process to identify risks that could impede efficient and effective achievement of organizational business process objectives.

Recommendation 2: We recommend that the Chief Financial Officer conduct a risk assessment that provides a basis for responding to a defined objective.

Recommendation 3: We recommend that the Chief Financial Officer design a risk response to each analyzed risk so that risk is within the defined risk tolerance for the defined objective. The risk responses may include the following:

- Acceptance – No action is taken to respond to the risk based on the insignificance of the risk.
- Avoidance – Action is taken to stop the operational process or the part of the operational process causing the risk.
- Reduction – Action is taken to reduce the likelihood or magnitude of the risk.
- Sharing – Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.

Gap 2: Payroll Process Controls

Management controls were not properly design and implemented to address segregation of duties within payroll processing. We noted unauthorized personnel could have approved employee timesheets.

Recommendations

Recommendation 4: We recommend that the Chief Financial Officer design a control in the payroll process in response to the entity's objectives and risks to achieve an effective internal control system. Controls include the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and risks.

Recommendation 5: We recommend that the Chief Financial Officer design the appropriate type of control for addressing segregation of duties in the payroll process.

Recommendation 6: We recommend that the Chief Financial Officer design a control in the payroll process at various levels, enhancing the policies and procedures governing the approval of timesheets.

Recommendation 7: We recommend that the Chief Financial Officer design a control requiring segregation of duties in the payroll process that will prevent employee timesheets being approved by unauthorized personnel.

Gap 3: Control Activities for Information Systems

Control activities were not properly designed for GPO's information system security management. We noted user accounts were not timely removed from GPO's Business Information System after separation and a new user account was not provisioned appropriately.

Recommendations

Recommendation 8: We recommend that the Chief Information Officer design a control for the entity's information system in response to the entity's objectives and risks to achieve an effective internal control system.

Recommendation 9: We recommend that Chief Information Officer design a control in the entity's information system covering information processing objectives for operational processes.

Recommendation 10: We recommend that Chief Information Officer design a control over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology.

Recommendation 11: We recommend that Chief Information Officer design a control for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system.

Recommendation 12: We recommend that Chief Information Officer design a control over development and maintenance of information technology

Gap 4: Policies and Procedures and Periodic Review of Control Activities

Each business unit may not have documented policies and procedures. In addition, there is no formal process for periodically reviewing controls for continued relevance and effectiveness in achieving the GPO's objectives or addressing related risks. We noted that all 34 SOPs reviewed were last updated in 2010.

Recommendations

Recommendation 13: We recommend that the Chief Financial Officer document responsibilities through policies and in the appropriate level of detail that will allow management to effectively monitor the control activity.

Recommendation 14: We recommend that the Chief Financial Officer conduct a periodic review of controls by developing a process for periodically reviewing policies, procedures, and related control activities for continued relevance and effectiveness in achieving GPO's objectives or addressing related risks.

Management's Response

Management concurred with the recommendations. The complete text of management's response is in Appendix C.

Appendix A – Objectives, Scope, and Methodology

The purpose of this assessment is to make recommendations for improvement for the areas upon which internal control oversight and risk management should be focused.

The following four *Green Book* principles were determined to be in scope for the purpose of the analysis.

- Principle 7—Identify analyze, and respond to risks
- Principle 10—Design control activities
- Principle 11—Design activities for the information system
- Principle 12—Implement control

Number	Principle Description	Scope Determination
1	Demonstrate Commitment to Integrity and Ethical Values	Out of Scope
2	Exercise Oversight Responsibility	
3	Establish Structure, Responsibility, and Authority	
4	Demonstrate Commitment to Competence	
5	Enforce Accountability	
6	Define Objectives and Risk Tolerances	
7	**Identify, Analyze, and Respond to Risks**	**In Scope**
8	Assess Fraud Risk	Out of Scope
9	Identify, Analyze, and Respond to Change	
10	**Design Control Activities**	**In Scope**
11	**Design Activities for the Information System**	
12	**Implement Control Activities**	
13	Use of Quality Information	Out of Scope
14	Communicate Internally	
15	Communicate Externally	
16	Perform Monitoring Activities	
17	Evaluate Issues and Remediate Deficiencies	

To accomplish the gap analysis, a review was performed of existing documentation, such as GPO's Accounting Manual policies, GPO standard operation procedures (SOPs), process and workflow documents for financial reporting, if available, and past audited financial statements to gain an understanding of current internal controls over the financial reporting environment as well as how the selected *Green Book* principles were addressed. GPO's entity-wide internal controls identified per the above existing documentation were mapped to the *Green Book* components, principles, and attributes for which they correspond.

In addition, inquiries with key officials were conducted to obtain additional information on how the selected *Green Book* principles were addressed. If there was a *Green Book*

attribute not being addressed by a GPO internal control (i.e. a gap), it was discussed and confirmed with the following GPO officials.

Title	Process Areas
Chief Financial Officer	Finance and Accounting
Deputy Chief Financial Officer	Finance and Accounting
Chief Accounts Receivable and Collection	Accounts Receivable and Revenues
Customer Services Controller	Accounts Payable and Expenses
Chief Accounting Operations	Financial Reporting
Chief Cash Management Services	Payroll

The assessment was performed from September 12, 2017, to November 3, 2017. Included in this report are the observations and recommendations as a result of assessment based on the information made available and interviews carried out with select GPO officials. The objective of this assessment does not include or support expressing an opinion on the design or effectiveness of GPO's internal control.

Appendix B – Acronyms

GAO	Government Accountability Office
GPO	U.S. Government Publishing Office
OIG	Office of Inspector General
SOP	Standard Operating Procedure

Appendix C - Management's Response

ANDREW M. SHERMAN
Chief of Staff

GPO

Date: February 2, 2018

To: Inspector General

Subj: Management Comments on OIG Draft Report No. 18-04, "Financial Management: Internal Controls Over Financial Reporting"

From: Chief of Staff

Thank you for the opportunity to review the subject draft report. Management concurs with the OIG recommendations contained in this report affecting GPO's Chief Financial Officer and Chief Information Officer (currently Acting), per the following:

Recommendation 1: We recommend that the Chief Financial Officer develop and implement a process to identify risks that could impede efficient and effective achievement of organizational business process objectives.

Response: Concur. The Office of Finance's organizational business process objectives are:

- Compliance with statutory requirements pertaining to accounting and budgeting requirements established in Titles 31 and 44;
- Provide fund control;
- Reliability of financial reporting, fair presentation, and disclosure of financial information;
- Provide cost-based budgeting;
- Enable the measurement of performance; and,
- Ensure proper stewardship of GPO assets.

As risk assessments of business processes are performed, process objectives and associated risks will be identified and system risks and process impediments will be evaluated against these objectives. This recommendation will be implemented in FY 2018 when the first risk assessment is scheduled. It will be continued in subsequent assessments.

Recommendation 2: We recommend that the Chief Financial Officer conduct a risk assessment that provides a basis for responding to a defined objective.

Response: Concur. Risk assessments will be conducted on an on-going basis so that systems are reviewed at least every three years. As part of this process, risks will be assessed and they will form the basis for designing the appropriate risk response. The assessments will include an evaluation of the system's achievement of process objectives. This recommendation will be implemented in FY 2018 when the first risk assessment is scheduled. It will be continued in subsequent assessments.

Recommendation 3: We recommend that the Chief Financial Officer design a risk response to each analyzed risk so that risk is within the defined risk tolerance for the defined objective.

Response: Concur. This step will be included as part of each risk assessment. Risk responses will be designed to address each analyzed risk, with consideration of risk tolerance. This recommendation will be implemented in FY 2018 when the first risk assessment is scheduled. Assessments will include a risk response for each risk identified. This process will be continued in subsequent assessments.

Recommendation 4: We recommend that the Chief Financial Officer design a control in the payroll process in response to the entity's objectives and risks to achieve an effective internal control system. Controls include the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and risks.

Response: Concur. A number of agency directives establish policy, while most payroll processes are documented in webTA and NFC (National Finance Center) procedural handbooks. Annually, these processes are audited by GPO's financial auditors. However, an overall processes flow and additional testing will be included in a risk assessment of webTA/Payroll processes. That assessment is scheduled in FY 2018.

Recommendation 5: We recommend that the Chief Financial Officer design the appropriate type of control for addressing segregation of duties in the payroll process.

Response: Concur. The standard webTA roles were reviewed and redesigned in the recent upgrade to provide clear separation of duties and responsibilities. An assessment of these roles will be part of the risk assessment of webTA/Payroll processes.

Recommendation 6: We recommend that the Chief Financial Officer design a control in the payroll process at various levels, enhancing the policies and procedures governing the approval of timesheets.

Response: Concur. The webTA upgrade addressed the issue: procedural controls have been put in place to govern the time sheet approval process. They are:

- The timesheet cannot be certified until the Friday before the end of a pay period. The system is configured to prevent earlier certification. However, in the event of unforeseen events (such as a furlough), the webTA Administrators (a restricted role) have the ability to open the system to allow for earlier certification.
- Employee's timesheets can be certified by the immediate supervisor or his or her delegate, or the Master Timekeeper only. If an employee enters leave that has not been requested and approved, the system sends the supervisor a warning to ensure that they review the leave posted on the time sheet before they certify the leave.
- Certification was changed to include a two-step process that now includes an attestation by those that enter their own leave and validate. Finance is looking into the addition of the second step for all agency employees. This will be included as part of the webTA risk assessment to be conducted in FY 2018.

An assessment of the timesheet approval process will be part of the risk assessment of webTA/Payroll system.

Recommendation 7: We recommend that the Chief Financial Officer design a control requiring segregation of duties in the payroll process that will prevent employee timesheets being approved by unauthorized personnel.

Response: Concur. The risk assessment of webTA/Payroll will include an assessment of the risk of unauthorized approval and the effectiveness of the separation of webTA duties in controlling unauthorized approval.

Recommendation 8: We recommend that the Chief Information Officer design a control for the entity's information system in response to the entity's objectives and risks to achieve an effective internal control system.

Response: Concur. The CIO has designed a control for this in the form of the System Security Plan for the entity's information system (GBIS) for internal controls for IT security risk and IT controls in accordance with the GPO IT Security Program Statement of Policy (GPO Directive 825.33B). This recommendation has been implemented.

Recommendation 9: We recommend that the Chief Information Officer design a control in the entity's information system covering information processing objectives for operational processes.

Response: Concur. The CIO has designed a control for this in the form of the System Security Plan for the entity's information system in accordance with the GPO IT Security Program Statement of Policy (GPO Directive 825.33B) which includes and covers operational processes. This recommendation has been implemented.

Recommendation 10: We recommend that the Chief Information Officer design a control over the information technology infrastructure to support the completeness, accuracy, and validity of information processing by information technology.

Response: Concur. The CIO has designed and implemented controls for the information technology infrastructure in the form of the System Security Plan and standard operating procedures for the General Support System (GSS) at GPO in accordance with the GPO IT Security Program Statement of Policy (Directive 825.33B) for this. The GSS Contingency Plan and GSS Contingency testing results aspects of this continue to be enhanced and are in work by IT and are expected to be completed by August 1, 2018.

Recommendation 11: We recommend that the Chief Information Officer design a control for security management of the entity's information system for appropriate access by internal and external sources to protect the entity's information system.

Response: Concur. Controls for security management of the entity's information system have been defined by GPO in the form of the System Security Plan for the information system, the

GPO IT Security Program Statement of Policy (GPO Directive 825.33B), and the GBIS Access Request Procedure on the GPO Intranet (which uses the IT Service Desk system).

GPO is processing an update to the GPO IT Security Program Statement of Policy Directive, to make even more explicit that GPO managers and supervisors must notify IT in a timely fashion via request submission to the IT Service Desk system when personnel leave GPO, so that the person's access can be removed by IT in a timely manner. The secondary control process in effect and operational using the Human Capital Office separation report notification can, as it did for this one account in this annual period, result in retroactive Separation Date from the Human Capital Office to IT, which resulted in the only discrepancy in the 2017 annual period. New user provisioning controls, policy and procedures exist and are comprehensive.

The single exception for new user provisioning noted during the annual review period was due to human procedural error and to address this, retraining of the personnel involved in this discrepancy and emphasis on following existing procedures has been completed. The update to the GPO IT Security Program Statement of Policy Directive is scheduled to be completed through the agency Directive approval process and implemented by May 1, 2018.

Recommendation 12: We recommend that the Chief Information Officer design a control over the development and maintenance of information technology.

Response: Concur. The CIO has designed and implemented controls over the development and maintenance of information technology (IT) in the form of the GPO IT Configuration Management (CM) Policy (GPO Directive 825.8). There are also specific controls for the development and maintenance of the entity's information system (GBIS) in the form of Request for Change (RFC) requests, reviews and approvals. This recommendation has been implemented.

Recommendation 13: We recommend that the Chief Financial Officer document responsibilities through policies and in the appropriate level of detail that will allow management to effectively monitor the control activity.

Response: Concur. This recommendation will be implemented in FY 2018.

- The Finance Policy Manual will be updated to include additional requirements for risk assessments.
- An inventory of existing Standard Operating Procedures (SoP's) will be completed. These will be reviewed and either be certified as current, or designated for revision.
- Completion of a gap analysis of SoP's will be completed.
- The outdated SOP's and those identified in the gap analysis will be assessed for risk and scheduled for future update.

Recommendation 14: We recommend that the Chief Financial Officer conduct a periodic review of controls by developing a process for periodically reviewing policies, procedures, and related control activities for continued relevance and effectiveness in achieving GPO's objectives or addressing related risks.

Response: Concur. This recommendation will be implemented in FY 2018. The Finance Policy Manual will be updated to include a policy for annual review of policies, cyclical review of SoP's and cyclical risk assessments of financial systems.

Thank you again for the opportunity to review the subject draft report. If you need additional information, please do not hesitate to contact me on 202-512-1100.

AM Sherman

ANDREW M. SHERMAN

Appendix D - Status of Recommendations

Recommendation	Resolved	Unresolved	Open/ECD*	Closed
1	x		FY 2018	
2	x		FY 2018	
3	x		FY 2018	
4	x		FY 2018	
5	x		TBD	
6	x		FY 2018	
7	x		TBD	
8	x		TBD	
9	x		TBD	
10	x		August 1, 2018	
11	x		May 1, 2018	
12	x		TBD	
13	x		FY 2018	
14	x		FY 2018	

*Estimated Completion Date.

Appendix E – Report Distribution

Acting Director, GPO
Chief of Staff
Chief Administrative Officer
Acting General Counsel

Major Contributor to the Report

Tony Temsupasiri – Lead Information Technology Specialist