



February 26, 2010

STEVEN R. PHELPS
MANAGER, SOX MANAGEMENT CONTROLS AND INTEGRATION

HAROLD E. STARK
MANAGER, SOX AND PROCESS IMPROVEMENT

SUBJECT: Audit Report – Postal Service Sarbanes-Oxley Information Technology
Fiscal Year 2009 Preparatory Testing
(Report Number FT-AR-10-011)

This report presents the results of our assessment of the U.S. Postal Service's testing of Sarbanes-Oxley (SOX) information technology (IT) controls (Project Number 09BM001FT003). This self-initiated review addresses financial and strategic risks and allows management to enhance the Postal Service's preparations for compliance with the Sarbanes-Oxley Act of 2002¹ in fiscal year (FY) 2010. The objective of our review was to determine how the Postal Service could improve its approach to testing key IT controls in preparation for this compliance. See [Appendix A](#) for additional information about this audit.

Conclusion

Management could strengthen its approach to testing key IT controls for compliance with SOX Section 404 provisions. When we conducted our fieldwork, we noted that:

- Management had not implemented procedures to facilitate coordination between the Business SOX Program Management Office (Business SOX PMO) and the Information Technology SOX Program Management Office (IT SOX PMO) when one group relies on compensating controls of the other. For example, the IT SOX PMO relied on revenue reconciliation business process controls to mitigate risks for two applications it determined would not be upgraded due to age, distribution, and cost of improving the technology. However, testing has shown that, to date, these controls are not effective. When business controls are not effective and would not compensate for identified IT risks, it is essential the IT SOX PMO and

¹ The U.S. Congress enacted SOX legislation in calendar year 2002 to strengthen public confidence in the accuracy and reliability of financial reporting. Section 404 of SOX requires management to state its responsibility for establishing and maintaining an adequate internal control structure and make an assertion on the effectiveness of the internal control structure over financial reporting. The Postal Accountability and Enhancement Act (PAEA) of 2006 mandates the Postal Service comply with Section 404 of SOX.

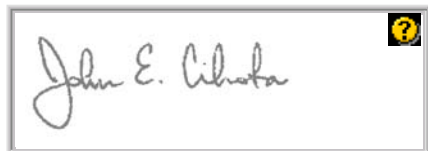
Business SOX PMO coordinate more closely while developing risk mitigation plans (RMPs) to learn which controls are not reliable and take other action.

- Management could improve the design, performance, and documentation of key IT control tests for the FY 2010 SOX compliance efforts. During our observations of operating effectiveness testing, we identified several areas for improvement. For example, the test teams could improve how they document test results as well as ensuring that testers are properly approved to use remote testing techniques when appropriate.

During discussions with the IT SOX PMO, management indicated that in FY 2010, the testers would review compensating controls identified in the RMPs and assess whether responsible parties tested the controls and determined them to be reliable. Further, management generally agreed with our results relating to the internal testing of key controls. They provided information on the actions they have implemented as they execute the FY 2010 testing cycle. Therefore, we are not making any recommendations at this time. However, we will continue to monitor these concerns in our FY 2010 SOX compliance audit. See [Appendix B](#) for a detailed discussion of this issue.

Since we did not make any recommendations in this report, management chose not to respond formally to this report.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Lorie Nelson, director, Financial Reporting, or me at (703) 248-2100.



John E. Cihota
Deputy Assistant Inspector General
for Financial Accountability

Attachments

cc: Joseph Corbett
Vincent H. DeVito, Jr.
John T. Edgar
Sally K. Haring

APPENDIX A: ADDITIONAL INFORMATION

BACKGROUND

The United States Congress enacted SOX legislation in 2002 to strengthen public confidence in the accuracy and reliability of financial reporting. The PAEA² mandates that the Postal Service comply with Section 404 of SOX. Section 404 requires management to state its responsibility for establishing and maintaining an adequate internal control structure and make an assertion on the effectiveness of the internal control structure over financial reporting.

The Postal Service spent FY 2009 designing and formalizing a control structure for the business processes that support Postal Service customers and partners, as well as IT controls to support processing operations. The IT SOX PMO performed operating effectiveness testing as a part of its responsibility to manage the design, development, and implementation of internal SOX master control standards for IT SOX compliance. The IT SOX PMO designed the control tests – including those observed by the U.S. Postal Service Office of Inspector General (OIG) – to measure the effectiveness of IT controls supporting accurate and reliable financial data processing.

OBJECTIVE, SCOPE, AND METHODOLOGY

The objective of our review was to determine how the Postal Service could improve its approach to testing key IT controls in preparation for compliance with provisions of the SOX Act of 2002. Our work included a review of the Postal Service's IT master controls and test instructions, an evaluation of all approved RMPs, an observation of control tests performed by Postal Service, and a review of final test documentation.

As of June 12, 2009, the Postal Service had approved eight RMPs documenting their strategy for addressing IT control gaps. As of September 25, 2009, the Postal Service had identified 248 IT master controls. Each master control could be applied a number of times across platforms, operating systems, applications, or databases in order to determine the number of associated detail controls. As a result, management estimated that about 2,500 detail controls would need testing.

We included 44 of the 248 IT master controls in our review. We conducted observations of the Postal Service test teams and documentation reviews of test evidence, analyses, and conclusions prepared by the test teams for 31 of the controls. We used judgmental selection criteria, which we based on the timing of the tests and our desire to observe a variety of controls. We also reviewed test documentation for 13 controls that we did not

² Public Law 109-435, signed on December 20, 2006.

observe. Our review of all test documentation was limited to the information exported from the GRCm tracking software³ by the IT SOX PMO.⁴

Members of Postal Service test teams in Eagan, MN, Raleigh, NC, and a roving team covering Postal Service Headquarters and various other processing locations performed the IT control tests. The OIG observed at least 20 percent of the master control tests each team conducted by the target dates listed in the table below. We focused on providing a range of coverage for the test of 248 master IT controls considered, rather than the approximately 2,500 detail control tests.

IT Control Tests Observed and/or Reviewed by OIG

Postal Service Team	Number of Control Tests Observed by OIG	Percentage of Controls Available for Observation⁵	Date Postal Service Completed Testing
Eagan	12	52%	9/11/2009
Raleigh	10	29%	9/11/2009
Roving	9	30%	9/25/2009
Subtotal	31		
Sample Application	Number of Control Tests Reviewed by OIG	Percentage of Controls Available for Review	Test Data Available As Of
TCSS	13 ⁶	50% ⁷	10/13/2009
Total tests discussed in report	44		

The control tests observed and test documentation reviewed by OIG covered about half of the IT systems and infrastructure components supporting the FY 2009 financial statements.

We conducted this self-initiated review from March 2009 through February 2010 in accordance with generally accepted government auditing standards and included such

³ Governance, Risk and Compliance Manager (GRCm) is the software the Postal Service uses to track and document its SOX testing of internal controls.

⁴ The Postal Service has not completed development and testing of read-only access to GRCm, so the OIG was not able to independently identify and select data for review.

⁵ We rounded percentages to the nearest whole number.

⁶ Two of the 15 TCSS controls had already been included in the tests observed as part of the Eagan and roving test teams controls.

⁷ This percentage represents 13 unduplicated controls of 26 total TCSS controls for which test data was available.

tests of internal controls as we considered necessary under the circumstances. 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 objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management officials on January 26, 2010, and included their comments where appropriate. We did not rely on computer-generated data to support the opinions and conclusions presented in this report.

PRIOR AUDIT COVERAGE

The OIG did not identify any prior audits or reviews related to the objective of this audit.

APPENDIX B: DETAILED ANALYSIS

Reliance on Business Controls

We reviewed all eight RMPs management had approved as of June 12, 2009, and found that compensating business controls that serve to mitigate IT risks in two RMPs might be unreliable. The business controls cited in the two RMPs relied on the effectiveness of the revenue reconciliation process at Postal Service field offices. However, the OIG reported concerns regarding reconciliations in its FY 2009 capping report of financial installation audits conducted at post offices, stations, and branches.⁸

According to Section 404 of SOX, management must document, test, and report on the operating effectiveness of internal controls over financial reporting on an ongoing basis. The Postal Service's *IT SOX Handbook*⁹ outlines Section 404 readiness activities to include testing the designated compensating controls for those IT SOX controls for which management has documented an RMP.

When notified of these concerns, IT SOX management indicated they did not coordinate with the Business SOX PMO when developing their risk mitigation plans. Targeted coordination between the two groups would help both Business SOX PMO and IT SOX PMO management better identify and address compensating business controls prior to SOX testing. As a result, management would have a more comprehensive understanding of the actions needed to address potential gaps in risk mitigation and control testing.

The two RMPs describe IT controls that are not in place for two applications due to the age, distribution, and costs associated with upgrading the technology used. Both RMPs point to the same set of 13 business controls to mitigate risks associated with the missing IT controls. Management described these business controls in Business Process Narratives (BPNs) related to retail sales units and cash deposits.¹⁰ These compensating controls relate to supervisory reviews and reconciliations over the financial reporting provided by field units. Specifically, field accounting procedures¹¹ require miscellaneous expenses to be issued to corresponding field units when exceptions are identified during reconciliations. Field accounting returns these exceptions to the field units for research and resolution. In FY 2009, the OIG found that 56 of 105 field units sampled did not monitor or resolve differences as required by Postal Service policy. As a result, business controls designed to ensure accurate financial reporting do not adequately mitigate the risks associated with missing IT master controls for IRT and POS units.

⁸ The OIG reported these issues in several capping reports, most recently in *Fiscal Year 2009 Financial Installation Audits – Post Offices, Stations, and Branches* (Report Number FF-AR-10-045, dated December 14, 2009).

⁹ *IT SOX Handbook*, June 2009, current as of November 2009.

¹⁰ BPN 102: ReSA – Retail Units, BPN 123: Cash Deposits – Bank of First Deposit/Wells Fargo, and BPN 124: Cash Deposits – Confirmed Deposits.

¹¹ Handbook F-101 *Field Accounting Procedures*, July 2008, with revisions through July 2009.

Subsequent to our review of RMPs, the IT SOX PMO performed tests in October of the IT controls included in one of the RMP's discussed above and concluded that the IT controls failed. The record of testing documented exceptions with some of the compensating business controls and identified other business controls the Business SOX PMO had not tested. In August, the IT SOX PMO also adjusted their approach to testing database layer controls for field applications such as POS. As a result, they determined that the second RMP discussed above was no longer necessary. Finally, the IT SOX PMO indicated that in FY 2010, testers will review compensating controls identified in the RMPs and assess whether responsible parties tested the controls and determined them to be reliable.

Internal Testing of Key IT Controls

Our review of Postal Service's testing of selected key IT controls disclosed that 29 of 44¹² IT controls had issues concerning:

- The manner in which the tests were performed.
- The quality of the supporting documentation for the analyses performed.
- The design of the test instructions to address the control objective.
- The manner in which the test results were reflected in the GRCm tracking software.

These issues were present in the work of each of the three Postal Service test teams, as well as in the documentation for a sample application.¹³ Specifically, for 19 controls, we identified issues with the manner in which management performed the tests to assess the operating effectiveness of the control. For example, we observed the tester was not present at the location for certain aspects of one control test. In this case, the tester used remote meeting software to oversee the commands executed by a Postal Service staff member during the test. While this may be an acceptable practice under certain conditions, it is difficult to ensure the individual responsible for assessing the effectiveness of the control adequately observes all aspects of the test. The IT SOX PMO indicated they intend to have testers present at control tests and will provide test teams with guidance in FY 2010 on the use of remote meeting software under appropriate conditions.

We also identified issues with 13 controls regarding the quality of documentation to support control tests. In one case, instructions for the inactivity timeout control test for UNIX workstations identified three different types of workstations to be reviewed. The supporting test documentation did not provide a listing of the types of workstations included in the universe for sampling or in the test analysis. The screen shots we

¹² There were 248 IT master (key) controls as of the date of our review.

¹³ Transportation Contract Support System (TCSS).

obtained show at least two types of workstations were included in the test, but did not include screen shots related to the third type. The test documentation did not indicate if the third type was used in Raleigh and should have been tested. We believe that under similar circumstances the sampling procedures should ensure at least one of each type of item described in a control be included in the sample selected for review. The IT SOX PMO indicated agreement with this concern. They also noted that management used alternative sampling methods in FY 2009 for readiness purposes, while they will use formal sampling methods in FY 2010 for assurance purposes.

For eight controls, we identified concerns with whether the test management performed effectively addressed the control objective. In one case, the control objective for patch management stated that management should evaluate application-level software patches or releases for applicable commercial off-the-shelf packages at least semiannually and implement them when appropriate. The control test documentation indicated that one of four patch reviews concluded with a recommendation to install the patch. However, the tester did not determine whether management took action on this recommendation and, instead, focused only on patches that management implemented into production in FY 2009. While our review of the patch assessment suggests the patch review progressed to the testing phase, it is unclear why the patch was not installed or whether information on the patch implementation was not loaded to the appropriate documentation library. We believe the testing approach should include confirmation that management tested and moved to production the recommended patches, as appropriate. The IT SOX PMO agreed with this concern and indicated they have enhanced the test design to include confirmation on whether management has implemented a patch into production.

Finally, we identified six controls with concerns related to how management applied the outcome of the tests to the sample application and/or how they recorded the tests in the tracking software. For one control, the test of password expirations disclosed that a tester confirmed the password expiration period for regular users at the time of the test was 176 days, which exceeded the 90-day requirement. Since there was a plan in place to reduce the expiration period from 176 to 90 days by October 2009, the tester reported the test result as PASS even though he tested the control in July 2009. We believe the test results recorded in the tracking software should reflect the condition of the control at the time of testing and not an expected future condition. In our discussions with management, the IT SOX PMO disagreed, stating they determined the remediation approach, timeframe, and conclusion were proper in accordance with IT executive briefing directives. While we do not dispute the reasonableness of the remediation action taken, we maintain that test results should reflect the condition of the control at the time of testing. In this case, remediation was not complete and the control was not functioning as intended at the time testing occurred.

The *IT SOX Handbook* outlines Section 404 readiness activities such as operating effectiveness testing and remediation. It provides guidance on performing tests at IT organizations, assigning staff to perform control testing, developing and implementing

remediation action plans, and incorporating all relevant analyses in the overall aggregation of results.

Management did not intend the FY 2009 testing documentation to substitute for formal assurance. Instead, management, in some cases, performed testing to allow for exploration and process validation in anticipation of FY 2010 SOX compliance efforts. Nevertheless, while we understand the differences between management's testing approach in FY 2009 and their approach for FY 2010, management should continue to focus on ensuring the adequacy of testing methods and related documentation are in order for FY 2010 to determine reliably the operating effectiveness of internal controls over financial reporting.

During preliminary discussions with the IT SOX PMO, OIG provided a detailed listing of the 44 key controls included in our review and the corresponding issues identified. The IT SOX PMO provided comments on the areas of concern. Whether by direct agreement from the IT SOX PMO or through knowledge of changes in the Postal Service's approach for IT testing in FY 2010, we believe we have reached general agreement with the Postal Service regarding these concerns.