



U.S. ENVIRONMENTAL PROTECTION AGENCY

OFFICE OF INSPECTOR GENERAL



Controls Over EPA's Compass Financial System Need to Be Improved

Report No. 13-P-0359

August 23, 2013



Scan this mobile
code to learn more
about the EPA OIG.

Report Contributors:

Rudolph M. Brevard
Michael Goode
Sabrena Stewart
Eric Jackson
Gina Ross
Teresa Richardson

Abbreviations

AICPA	American Institute of Certified Public Accountants
CFO	Chief Financial Officer
EPA	U.S. Environmental Protection Agency
NIST	National Institute of Standards and Technology
OCFO	Office of the Chief Financial Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
QASP	Quality Assurance Surveillance Plan

Hotline

To report fraud, waste, or abuse, contact us through one of the following methods:

email: OIG_Hotline@epa.gov
phone: 1-888-546-8740
fax: 202-566-2599
online: <http://www.epa.gov/oig/hotline.htm>

write: EPA Inspector General Hotline
1200 Pennsylvania Avenue, NW
Mailcode 2431T
Washington, DC 20460



At a Glance

Why We Did This Review

We conducted this audit to determine what steps the U.S. Environmental Protection Agency took to ensure that internal controls over the financial reporting by Compass Financials have been designed appropriately and are operating effectively. We also sought to determine the extent of the EPA's reliance on its service organization to make assertions about the effectiveness of its internal controls over financial reporting. Additionally, we reviewed the EPA's oversight strategy for key Compass processes.

In October 2011, the EPA replaced its legacy financial management system. The new system, Compass, was developed and is currently hosted by a third party service provider. During fiscal year 2012, the EPA used Compass to produce its financial statements that were submitted to the Office of Management and Budget and Congress.

This report addresses the following EPA Goal or Cross-Cutting Strategy:

- *Strengthening EPA's workforce and capabilities.*

For further information, contact our Office of Congressional and Public Affairs at (202) 566-2391.

The full report is at:
www.epa.gov/oig/reports/2013/20130823-13-P-0359.pdf

Controls Over EPA's Compass Financial System Need to Be Improved

What We Found

Processes were not in place to monitor performance of the EPA Office of the Chief Financial Officer's third party service provider of Compass. Also, OCFO security personnel were not aware of Compass security roles and responsibilities. This lack of oversight:

- Inhibits the EPA's ability to achieve agreed-upon performance levels and correctly pay for services rendered.
- Decreases the likelihood that an effective security posture will be maintained.

Further, disaster recovery exercise plans did not include testing of data replication processes critical to financial reporting, resulting in the EPA having no assurance that Compass will operate as designed during a disaster.

Recommendations and Planned Agency Corrective Actions

We recommended that the Chief Financial Officer develop a process to monitor and evaluate, on a monthly basis, the service provider's performance and adjust service level requirements accordingly. Further, we recommended that the CFO communicate key roles and responsibilities to designated security personnel, and test Compass data replication during a functional disaster recovery exercise.

OCFO did not agree with our recommendations in the draft report. We met with and reviewed documentation provided by OCFO related to recommendations 1 through 3. Our review determined that OCFO made progress in addressing our findings related to management oversight of service provider performance and the OIG has agreed to amend recommendations 1 through 3 to reflect this progress. The OIG also considers corrective actions taken by OCFO prior to the issuance of the draft report in response to recommendation 4 to be sufficient to close this recommendation. We also amended recommendation 5 to reflect agreed-upon alternative corrective actions that OCFO should take to address our findings related to Compass disaster recovery. OCFO concurred with these changes.

After these amendments, we recommended that the CFO finalize internal procedures used for reviewing the service provider's performance, continue to review service provider performance on a monthly basis and document results of the monthly meetings, finalize the revised Quality Assurance Surveillance Plan that includes revised service level requirements to accurately assess service provider performance, and test inherent Compass financial reporting capabilities during a functional disaster recovery exercise.



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

THE INSPECTOR GENERAL

August 23, 2013

MEMORANDUM

SUBJECT: Controls Over EPA's Compass Financial System Need to Be Improved
Report No. 13-P-0359

FROM: Arthur A. Elkins Jr.

A handwritten signature in cursive script, appearing to read "Arthur A. Elkins Jr.", is written over the printed name.

TO: Maryann Froehlich, Acting Chief Financial Officer

This is our report on the subject audit conducted by the Office of Inspector General of the U.S. Environmental Protection Agency. This report contains findings that describe the problems the OIG identified and the corrective actions the OIG recommends. This report represents the opinion of the OIG and does not necessarily represent the final EPA position. The EPA agreed with all five recommendations. These recommendations are considered unresolved pending our receipt of the EPA's corrective action plan and estimated completion dates.

Action Required

In accordance with EPA Manual 2750, you are required to provide planned corrective actions and completion dates for all unresolved recommendations within 60 calendar days. Your response will be posted on the OIG's public website, along with our memorandum commenting on your response. Your response should be provided as an Adobe PDF file that complies with the accessibility requirements of Section 508 of the Rehabilitation Act of 1973, as amended. The final response should not contain data that you do not want to be released to the public; if your response contains such data, you should identify the data for the redaction or removal along with corresponding justification. We will post this report to our website at <http://www.epa.gov/oig>.

If you or your staff have any questions regarding this report, please contact Richard Eyermann at (202) 566-0565 or eyermann.richard@epa.gov, or Rudolph M. Brevard at (202) 566-0893 or at brevard.rudy@epa.gov.

Table of Contents

Chapters

1	Introduction	1
	Purpose	1
	Background	1
	Scope and Methodology	1
2	Management Oversight of Compass Service Provider Needs Improvement	3
	OCFO Does Not Have a Process to Evaluate Service Provider Performance.....	3
	Recommendations	4
	Agency Response and OIG Evaluation	4
3	Compass Security and Disaster Recovery Process Improvements Needed.....	6
	Lack of Knowledge of Key Security Processes Inhibits EPA's Ability to Handle Risks	6
	Critical Data Replication Function Not Tested for Contingency Operations	6
	Recommendations	7
	Agency Response and OIG Evaluation	7
	Status of Recommendations and Potential Monetary Benefits.....	9

Appendices

A	Agency Response to Draft Report.....	10
B	Distribution	13

Chapter 1

Introduction

Purpose

The Office of Inspector General of the U.S. Environmental Protection Agency conducted this audit to determine what steps the EPA took to ensure that internal controls over the financial reporting by Compass Financials have been designed appropriately and are operating effectively. We also sought to determine the extent of the EPA's reliance on its service organization to make assertions about the effectiveness of its internal controls over financial reporting. Further, we reviewed the agency's strategy for overseeing key Compass processes.

Background

In October 2011, the EPA's Office of the Chief Financial Officer replaced its legacy financial management system (the Integrated Financial Management System) with a new system—Compass. Compass was developed and is hosted by a third party service provider. The EPA indicated the objectives of Compass are to:

- Achieve or enhance process improvements and cost savings in the acquisition, development, implementation, and operation of financial management systems through shared services, joint procurements, consolidation, and other means.
- Provide for standardization of business processes and data elements.
- Promote seamless data exchange between and among federal agencies.
- Strengthen internal controls through real-time interoperability of core financial and subsidiary systems.

Scope and Methodology

We performed this audit from February 2012 to May 2013 at EPA headquarters in Washington, D.C., and at the third party service provider's data center in Phoenix, Arizona. We performed this audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on the audit objectives.

We conducted the review of Compass key processes and its third party service provider's expected service level goals. Further, we reviewed the agency's strategy for monitoring the third party service provider's performance. We also reviewed steps taken to ensure that internal controls over financial reporting have been designed appropriately and are operating effectively.

Our criteria included agency security plans and policies and the National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*. The evaluation of these controls and agency guidance were carried out through inquiry, observation, and review of documentation.

We identified issues during this audit regarding the ability of the agency's Compass service provider to assess the design and operating effectiveness of controls over business processes affecting the EPA. We reported them in EPA OIG Report No. 13-1-0054, *Audit of EPA's Fiscal 2012 and 2011 Consolidated Financial Statements*, because of the potential impact these issues could have on the agency's ability to conduct reliable financial reporting. Since the publishing of the agency's financial statement audit report, OCFO has concurred with our findings in this area and is in the process of taking steps to address the deficiencies noted.

Chapter 2

Management Oversight of Compass Service Provider Needs Improvement

Internal agency processes were not in place to monitor performance of OCFO's third party service provider for Compass. Federal and agency guidance requires the timely review and monitoring of a service provider's performance. This lack of oversight inhibits the EPA's ability to achieve agreed-upon performance levels and correctly pay for services rendered.

OCFO Does Not Have a Process to Evaluate Service Provider Performance

OCFO had not established an internal process for how it would conduct a review of service provider performance. Though OCFO had a QASP in place that stated that it would review service provider performance, the EPA had not documented how its internal review process would be performed. OCFO only asserted that it had assembled a team of OCFO personnel to review service provider performance, but roles and responsibilities had not been determined. Office of Management and Budget Circular A-127, *Financial Management Systems*, states that agencies must monitor their service providers' performance. The EPA's *Contracts Management Manual* also states that the program office's contracting officer's representative is responsible for overseeing contractor performance and notifying the contracting officer as to whether the contractor met established performance standards. Lack of documented internal procedures for the EPA's review of its service provider inhibits the EPA's ability to ensure that the service provider internal reviews are conducted in a manner consistent with EPA policy and executive branch directives.

Proposed Quarterly Review Not Timely

At the time of this review, OCFO had not documented an internal process to review service provider performance. However, OCFO has discussed reviewing service provider performance on a quarterly basis. We were encouraged that OCFO had begun to discuss how it will review contractor performance, but this review must occur more frequently. OMB Circular A-127 states that agencies must ensure that service failures are resolved promptly. In addition, EPA's *Contracts Management Manual* requires a monthly review of a contractor's progress reports. Limiting the review of performance to a quarterly basis increases the risk that oversight of performance will not be timely.

Service Level Requirements Have Not Been Adjusted

OCFO and its service provider had not adjusted service level requirements by the end of the burn-in period as agreed. OCFO uses the service level requirements to measure service provider performance. Service level requirements are also used to calculate penalties for nonperformance. OCFO agreed to a 6-month burn-in period in which the EPA and its service provider would work together to review performance thresholds and measurement methods, and make adjustments as necessary. The EPA agreed not to assess penalties during the burn-in period. After the burn-in period, OCFO agreed to measure its service provider's performance based on the adjusted service level requirements metrics. The burn-in period has ended and OCFO and its service provider are still reviewing the service level requirements. OCFO anticipates reducing the number of service level requirements to refine the performance metrics and better assess where penalties can be applied. However, by not having adjusted service level requirements in place by the end of the burn-in period, OCFO cannot accurately measure and evaluate its service provider's performance.

We met with OCFO representatives to discuss our findings related to oversight of the service provider's performance. OCFO management stated that they assembled a team to conduct performance reviews. OCFO also submitted to the audit team an informal standard operating procedure for reviewing service provider performance. Our review of the information provided by OCFO disclosed that while the agency started taking steps to review the service provider's performance, management had not yet finalized its processes or documented the results of its monthly meetings.

Recommendations

We recommend that the chief financial officer:

1. Finalize internal procedures used for reviewing the service provider's performance.
2. Continue to review service provider performance on a monthly basis and document results of the monthly meetings.
3. Finalize the revised Quality Assurance Surveillance Plan that includes the revised service level requirements to accurately assess service provider performance.

Agency Response and OIG Evaluation

OCFO initially disagreed with our recommendations regarding service provider performance. OCFO stated they did not believe the draft report accurately reflected the state of the EPA's oversight of the service provider. OCFO

specifically noted that the draft report did not acknowledge that the EPA had a QASP that outlines its oversight procedures. While the EPA had a QASP, roles and responsibilities had not been determined for the team responsible for performing oversight nor had formalized processes been developed to ensure consistent review of the service provider's performance. However, we updated the report to acknowledge the existence of the QASP. Furthermore, we met with and reviewed additional documentation provided by OCFO related to their disagreement with recommendations 1-3. Our review of provided documentation determined that OCFO has made progress in addressing our findings related to management oversight of service provider performance and the OIG agreed to amend recommendations 1 - 3 to reflect this progress. OCFO concurred with these changes.

Chapter 3

Compass Security and Disaster Recovery Process Improvements Needed

OCFO security personnel were not aware of Compass security roles and responsibilities. Federal guidance states that a management official knowledgeable in the nature of the information should be assigned security responsibilities for each major application. This lack of knowledge greatly decreases the likelihood that an effective security posture will be maintained. Also, disaster recovery exercises did not test data replication processes vital to financial reporting. Federal guidance states that contingency plan testing should be conducted in real or near-real time, to allow participants to carry out their roles and responsibilities as realistically as possible. Without conducting disaster recovery testing that includes all components, the EPA cannot be assured that Compass will operate as designed during a disaster.

Lack of Knowledge of Key Security Processes Inhibits EPA's Ability to Handle Risks

OCFO has defined system security processes for Compass, but staff assigned key system security duties were not knowledgeable about processes, roles, and responsibilities. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, states that responsibility for security should be assigned to those knowledgeable in the nature of those security tasks assigned to them. When we interviewed personnel responsible for Compass security incidents, they were unable to convey how security incidence responses are handled or identify their role and responsibilities within the process. Also, some of the personnel who were documented in the Compass system security plan as having assigned security roles were unaware that they were listed in the system security plan or that they were points of contact for the oversight of key security controls. Lack of knowledge regarding security roles and responsibilities could result in the ineffective design and operation of Compass security controls.

Critical Data Replication Function Not Tested for Contingency Operations

OCFO did not include data replication in its Compass disaster recovery testing plans. Financial data entered into Compass is replicated from the Compass hosting location to the EPA's Research Triangle Park data center. The replicated data feed the Compass Data Warehouse, which generates the agency's financial reports. If data replication is not functioning during a disaster, the Compass Data Warehouse cannot generate financial reports. The Contingency Plan and Exercise

section within NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, states that organizations should demonstrate realistic test/exercise scenarios that effectively stress the information system and support the Agency's mission. In addition, NIST Special Publication 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, states that functional exercises are typically conducted in real or near-real time and prompt participants to carry out their roles and responsibilities as realistically as possible. Without including data replication testing in functional disaster recovery exercise plans, the EPA has no assurance that Compass will operate as designed during a disaster.

We met with OCFO representatives to discuss their concerns regarding our disaster recovery audit findings. OCFO representatives stated that disaster recovery exercise plans would still not include testing of Compass data replication and maintain that Compass has the ability to carry out reporting functions in the event of a disaster. As such, they maintain, that testing data replication to the Compass data warehouse is not necessary. However, if the EPA relies upon Compass reporting capabilities during a disaster, the agency should have a plan to test its capability. Our review of the EPA's disaster recovery results revealed that management had not taken steps to identify key Compass reports that require testing during disaster recovery exercises

Recommendations

We recommend that the chief financial officer:

4. Communicate key roles and responsibilities to designated security personnel.
5. Test inherent Compass financial reporting capabilities during a functional disaster recovery exercise.

Agency Response and OIG Evaluation

OCFO completed agreed upon corrective actions associated with recommendation 4 prior to the issuance of the draft report. The OIG considers corrective actions taken to be sufficient to address our findings and have closed this recommendation. OCFO did not agree with our recommendation to test the COMPASS data replication as part of the disaster recovery exercise. OCFO stated that data replication is not a mission-critical component of the agency's contingency planning and disaster recovery processes. We met with OCFO to discuss their concerns and reviewed the latest disaster recovery test results. While the EPA does not rely on data replication for its financial reporting capabilities during a disaster, management does rely upon the COMPASS inherent reporting capabilities during contingencies. As such, the OIG believes it is incumbent upon management to have a process to test the most critical COMPASS reporting

functions during disaster recovery exercises. As a result of our meeting, the OIG agreed to amend the recommendation to reflect agreed upon alternative corrective actions that OCFO should take to address our finding in this area. OCFO concurred with this change.

Status of Recommendations and Potential Monetary Benefits

RECOMMENDATIONS						POTENTIAL MONETARY BENEFITS (in \$000s)	
Rec. No.	Page No.	Subject	Status ¹	Action Official	Planned Completion Date	Claimed Amount	Agreed-To Amount
1	4	Finalize internal procedures used for reviewing the service provider's performance.	U	Chief Financial Officer			
2	4	Continue to review service provider performance on a monthly basis and document results of the monthly meetings.	U	Chief Financial Officer			
3	4	Finalize the revised Quality Assurance Surveillance Plan that includes revised service level requirements to accurately assess service provider performance.	U	Chief Financial Officer			
4	7	Communicate key roles and responsibilities to designated security personnel.	C	Chief Financial Officer	12/13/12		
5	7	Test inherent Compass financial reporting capability during a functional disaster recovery exercise.	U	Chief Financial Officer			

¹ O = recommendation is open with agreed-to corrective actions pending
 C = recommendation is closed with all agreed-to actions completed
 U = recommendation is unresolved with resolution efforts in progress

Agency Response to Draft Report

MEMORANDUM

SUBJECT: Response to the Office of Inspector General Draft Report No. OMS-FY12-0002 “Controls Over EPA’s Compass Financial System Need to Be Improved,” dated May 23, 2013

FROM: Maryann Froehlich
Acting Chief Financial Officer

TO: Arthur A. Elkins, Jr.
Inspector General

Thank you for the opportunity to respond to the issues and recommendations in the subject draft audit report. Following is a summary of the agency’s overall position, along with its position on each of the report recommendations. For the report recommendations with which the agency does not agree, we have explained our position and proposed alternatives to recommendations.

AGENCY’S OVERALL POSITION

We do not believe the draft report accurately reflects the state of EPA oversight of our service provider’s performance or the information provided to the auditors. We do not agree with recommendation numbers 1-3. Auditors, who met with my staff in the Office of Technology Solutions (OTS) last year, were informed that the initial process for reviewing service provider performance was going to be changed. The draft report does not acknowledge that there was, *and is*, such a process as is defined in our Quality Assurance Surveillance Plan (QASP). We are in the midst of negotiating changes to the existing QASP that will modify our process for reviewing contractor performance. Even though these negotiations are still in progress, we are not without a QASP as the current QASP remains fully in effect and operative.

The QASP (provided to the auditors) documents the service level requirements to which the service provider is held. The service provider does submit monthly reports on these requirements and performance is discussed at monthly review meetings, as required in the *Contracts Management Manual*, contrary to the draft finding. The reference in the draft report regarding, “reviewing service provider performance on a quarterly basis,” is a documented evaluation in addition to the monthly review and informal feedback routinely provided to the service provider.

We do not agree with recommendation number 4 on communicating responsibilities to security personnel as this action was completed prior to issuance of the draft report. OTS, in a July 16, 2012, memorandum to the audit team, offered to provide refresher training on security roles and responsibilities to staff. When the training was held on December 13, 2012, OTS sent the audit

team an email on the same date that informed them that OTS personnel had been briefed on security roles/responsibilities and provided the audit team a copy of the training presentation.

We also do not agree with recommendation number 5 on testing data replication during a disaster recovery exercise. Mission-critical transactional data is maintained in the core financial system and this system is subject to contingency planning and disaster recovery. Since the data replication process represents the creation of a local copy of this transactional data, we submit that this process is not mission-critical and should not be included in disaster recovery exercises. OIG acknowledges that there is no requirement to include replication in disaster recovery and has not presented a reason to justify the allocation of scarce resources to do so.

AGENCY’S RESPONSE TO REPORT RECOMMENDATIONS

No.	Recommendation	Agency Explanation/Response	Proposed Alternative
1	Develop a process to monitor service provider performance.	EPA has a process in place and is negotiating changes to update it.	Complete and implement adjusted service level requirements to accurately assess service provider performance.
2	Review and evaluate service provider performance on a monthly basis.	Service provider performance is discussed at monthly meetings. We believe quarterly written evaluation is sufficient when combined with the monthly meetings.	Evaluate service provider performance on a quarterly basis. Continue reviewing performance at monthly meetings.
3	Adjust service level requirements to accurately assess service provider performance.	As noted above, EPA is in the process of making such adjustments. OIG was informed that this effort would occur.	Complete and implement adjusted service level requirements to accurately assess service provider performance.
4	Communicate key roles and responsibilities to designated security personnel.	EPA assigns certain security roles by signed memorandum. Additionally, OIG was informed on 12/13/12 of an Office-wide briefing on this subject.	Remove or acknowledge that corrective action was taken prior to the draft report.
5	Test Compass data replication during a functional disaster recovery exercise.	Replication is not mission-critical. The transactional system is key; reporting/feeder systems do not qualify for recovery.	Delete this recommendation.

We would welcome the opportunity to meet with OIG staff and discuss our concerns with the draft recommendations. If you have any questions regarding this response, please contact Quentin Jones, Director, Office of Technology Solutions, on (202) 564-0373 or Susan Lindenblad, OTS Audit Liaison, on (202) 566-2890.

cc: Richard Eyerman, Acting Assistant Inspector General for Audit
David Bloom Acting Deputy Chief Financial Officer
Joshua Baylson, Associate Chief Financial Officer
Quentin Jones, Director, Office of Technology Solutions
Robert Hill, Deputy Director, Office of Technology Solutions

Distribution

Office of the Administrator
Chief Financial Officer
Agency Follow-Up Coordinator
General Counsel
Associate Administrator for Congressional and Intergovernmental Relations
Associate Administrator for External Affairs and Environmental Education
Deputy Chief Financial Officer
Audit Follow-Up Coordinator, Office of the Chief Financial Officer