OFFICE OF INSPECTOR GENERAL

Audit Report

Audit of the Data Management Application Controls and Selected General Controls in the Financial Management Integrated System

Report No. 14-12
September 30, 2014

RAILROAD RETIREMENT BOARD

EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the Railroad Retirement Board (RRB) conducted an audit of data management application controls and selected configuration management, segregation of duties, and contingency planning general controls in the RRB's Financial Management Integrated System (FMIS). The objective of our audit was to assess the adequacy of the controls.

Background

In October 2013, the RRB transitioned from a mainframe based financial management system to FMIS, a web-based, cloud hosted system. Data management components of an application include the logical design and physical architecture of the system, and control the entry, storage, retrieval, and processing of information. In an effective internal control environment, configuration management controls should be in place to ensure adequate migration from an older system to a newer system; a contractor's organizational structure should have proper segregation of duties; and contingency planning should ensure the continuity of operations if an unplanned interruption of operation occurs.

Findings

Our audit determined that the FMIS controls for data management, configuration management (migration of the system), contractor segregation of duties, and contingency planning are adequate; however, some control deficiencies exist. We determined that the RRB should:

- create system specific procedures for access to the FMIS application;
- update the FMIS System Security Plan to correct errors in control descriptions and ensure missing controls are reflected; and
- modify audit and accountability procedures to reflect current practice.

Additionally, an official from the Bureau of Fiscal Operations notified us that the RRB anticipates migrating their Program Accounts Receivable system to one that will fully integrate with FMIS. Similar control deficiencies could occur during the course of that migration if lessons learned are not effectively applied.

Recommendations

We made eight recommendations to RRB management to address the control deficiencies that we identified in the audit.

Management's Response

The Bureau of Fiscal Operations concurred with three recommendations and partially concurred with two. They consider the Financial Management System Security Plan as

the primary vehicle for control language and information, and will update that plan after consulting with the FMIS contractor. They will also publish the necessary procedures for obtaining access to FMIS and provide the PAR migration team with the reported OIG findings and recommendations, as well as other lessons learned documentation from the FMIS migration.

The Bureau of Information Services concurred with the three recommendations addressed to their Bureau. They will review and modify the applicable policies and procedures.

TABLE OF CONTENTS

INTRODUCTION

This report presents the results of the Office of Inspector General's (OIG) audit of the application controls for data management and selected general controls for configuration management, segregation of duties, and contingency planning in the Railroad Retirement Board's (RRB) Financial Management Integrated System (FMIS).

Background

The RRB is an independent agency in the executive branch of the Federal government. The RRB administers the retirement/survivor and unemployment/sickness insurance benefit programs for railroad workers and their families under the Railroad Retirement Act and the Railroad Unemployment Insurance Act. The RRB paid $11.7 billion in retirement/survivor benefits and $84.5 million in unemployment and sickness insurance benefits during fiscal year 2013.[1]

The RRB uses its Financial Management System to record financial transactions and to support the preparation of the agency's annual financial statements. In October 2013, the RRB transitioned from the Federal Financial System, a mainframe based financial management system to FMIS, a web-based, cloud hosted system. FMIS, which is provided by a contractor for the RRB and is owned by the agency's Bureau of Fiscal Operations (BFO), was authorized to operate by the RRB's Chief Financial Officer on September 30, 2013. FMIS is the core system for budget formulation and execution, procurement, payment and receivable management, general ledger management, debt collection and external reporting. The other component application of the Financial Management System is the Program Accounts Receivable (PAR) system.

The Federal Information System Controls Audit Manual (FISCAM), developed by the Government Accountability Office (GAO), provides a methodology for evaluating information system controls.[2] FISCAM has specific control objectives with audit techniques and procedures for each of the control review areas to evaluate the effectiveness of the controls.

Data management components of an application include the logical design and physical architecture of the system, and control the entry, storage, retrieval, and processing of information. Additionally, in an effective internal control environment:

- configuration management controls should be in place to ensure adequate migration from an older system to a newer system;
- a contractor's organizational structure should have proper segregation of duties; and
- contingency planning should ensure the continuity of operations if an unplanned interruption of operation occurs.

[1] *Railroad Retirement Board Performance and Accountability Report*, Fiscal Year 2013.
[2] *Federal Information System Control Audit Manual (FISCAM)*, GAO-09-232G, February 2009.

This audit supports the RRB's strategic plan to "[s]erve as responsible stewards for our customers' trust funds and agency resources" and includes an objective to "ensure effectiveness, efficiency, and security of operations." This audit addresses controls that ensure security of operations.

This audit will also directly support the OIG's mandated annual Federal Information Security Management Act (FISMA) evaluation and indirectly support the OIG's audit of the RRB's financial statements.[3]

Audit Objective

The objective of this audit was to assess the adequacy of the data management controls and selected configuration management, segregation of duties, and contingency planning controls in FMIS.

Scope

The scope of the audit was October 2013 through June 2014, and configuration management controls over the system migration that took place in fiscal year 2013.

Methodology

To accomplish the audit objective, we:

- reviewed pertinent laws and guidance;
- reviewed pertinent RRB policies and procedures to ensure compliance with laws and guidance;
- reviewed documentation and interviewed responsible agency management and staff to gain an understanding of the internal controls placed into operation, including those for data management;
- reviewed the procedures used for obtaining access to FMIS;
- reviewed the system development process used for FMIS migration;
- reviewed the FMIS configuration management documentation to support acceptance testing and system migration;
- reviewed the contractor's organizational chart and access profiles to ensure access privileges are properly segregated;
- reviewed the procedures used for monitoring FMIS auditable events, including methods for detecting abnormal activity; and
- reviewed documentation to support the FMIS contingency plan.

[3] *Federal Information Security Management Act of 2002*, Public Law 107-347.

The primary guidance for this audit included FISCAM, FISMA, and the National Institute of Standards and Technology (NIST) standards and guidance.

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We conducted our fieldwork at the RRB's headquarters in Chicago, Illinois from January 2014 through July 2014.

RESULTS OF AUDIT

Our audit determined that the FMIS controls for data management, configuration management (migration of the system), contractor segregation of duties, and contingency planning are adequate; however, some control deficiencies exist. We determined that the RRB should:

- create system specific procedures for access to the FMIS application;
- update the FMIS System Security Plan (SSP) to correct errors in control descriptions and ensure missing controls are reflected; and
- modify audit and accountability procedures to reflect current practice.

Additionally, we were notified that the RRB anticipates migrating their PAR system to one which will fully integrate with FMIS. This migration could potentially result in similar deficiencies and risks.

The details of our findings and recommendations for corrective action follow.

Agency management generally concurs with our recommendations. The full texts of management's responses are included in Appendices I and II of this report.

Lack of System-Specific Procedures for Access to FMIS

There are no system-specific policies and procedures for acquiring access to FMIS. System-specific procedures for the Financial Management System were previously recommended in 2009, but have not yet been established. Additionally, the existing RRB general policies and procedures for access control are outdated and do not reflect the additional actions or notifications required to obtain access to the FMIS application. During the course of our audit, we observed that access requests for FMIS were not handled timely.

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires that agencies develop, document, and disseminate an access control policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. This guidance also requires that agencies review and update the current access control policy and procedures.

The FMIS application, implemented in October 2013, contains many more security roles and profiles than the Federal Financial System. The BFO FMIS administrator stated that he is still learning the system, which is a continuing process as implementation of the application continues. Presently, when an RRB employee requires access or a change in access, the BFO FMIS administrator reviews the access requested and will authorize the contractor to implement that access. In the future, the BFO FMIS administrator will implement the access without contractor assistance.

The RRB's Bureau of Information Services (BIS) is responsible for the general information security policies and procedures. The general policies and procedures for access controls refer to special access procedures for external systems. These policies and procedures are published in four RRB documents: (1) Administrative Circular, Information Resource Management-18, *Information Security Policy*; (2) Access Control Policy; (3) Access Control Processes and Procedures; and (4) Appendix A – RRB System Access Policy.

All of these documents state that there are some external systems that have special procedures for processing access requests; however, these documents do not include the Financial Management System (which consists of FMIS and the PAR system) as one of the external systems requiring special access procedures. The Chief Security Officer informed us that BIS has been working with a limited staff, which has caused some tasks such as reviewing, updating, and finalizing specific policies and procedures to be delayed. An additional employee is expected to begin work by the end of fiscal year 2014.

The lack of system-specific policies and procedures can result in improper or unprocessed requests for access to the FMIS application. There is an increased risk of security exposure and control gaps when policies and procedures are not reviewed and updated timely.

Recommendations

1. The Bureau of Fiscal Operations should ensure the BFO FMIS administrator acquires the expertise to implement access or changes in access without contractor assistance.

2. The Bureau of Fiscal Operations should implement system-specific procedures for obtaining access to FMIS.

3. The Bureau of Information Services should update the four general policy and procedure documents to include all systems requiring special access procedures.

Management's Responses

The BFO concurs with recommendations 1 and 2. For recommendation 1, they stated the FMIS administrator has acquired the expertise to make routine implementations and changes of access with the current security configuration supplied by the contractor, but will continue to rely on support from the FMIS helpdesk for assistance in any modifications to the current configuration.

The BIS concurs with recommendation 3. The Chief Security Officer will update (1) Administrative Circular, Information Resource Management (IRM)-18, *Information Security Policy*; (2) Access Control Policy; (3) Access Control Processes and Procedures, and (4) Appendix A – RRB System Access Policy to include all systems requiring special access procedures.

OIG's Comments on Management's Response

The OIG's intention with recommendation 1 is to ensure the FMIS administrator is able to implement access or changes in access without contractor assistance. This would include situations where new or modified security configurations may be required.

FMIS System Security Plan Needs Updating

Control descriptions within the FMIS SSP are inaccurate or incomplete for some controls and need to be updated. The FMIS SSP also needs to be updated to include additional controls required for moderate impact systems based on updates in NIST SP 800-53, Revision 4.

We identified the following inaccurate or incomplete control information within the FMIS SSP:

- Access to the FMIS application is inaccurately shown as controlled by the RRB Active Directory when it is not.
- The list of applicable policies referenced for configuration management is incomplete.
- Incomplete control descriptions suggest that the control is fully inherited by either the RRB or the contractor when they share responsibility for control implementation.
- New controls established in NIST SP 800-53, Revision 4, are not present in the FMIS SSP. There is a one year grace period from the publication date of April 2013 for the implementation of these new controls.

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems,* states that the SSP should be reviewed annually to ensure current information about the system. Federal Information Processing Standards Publication 200, *Minimum Security Requirements for Federal Information and Information Systems,* specifies the minimum security requirements as defined in NIST SP 800-53, Revision 4.

RRB management did not ensure that the correct control language was documented in the FMIS SSP. The contractor prepared the FMIS SSP for the RRB in September 2013, just prior to system migration. Additionally, the FMIS SSP was based on the recommended security controls outlined in NIST SP 800-53, Revision 3, as the one year grace period for implementing new controls in Revision 4 had not elapsed.[4]

Since FMIS is a web-based, cloud hosted system, and the responsibilities for information security controls are performed by the contractor and/or the RRB, and both

[4] *Recommended Security Controls for Federal Information Systems and Organizations*, NIST SP 800-53, Revision 3, August 2009.

the contractor and RRB have multiple organizations that perform these responsibilities, the RRB should maintain the following documents detailing the information security control environment for the Financial Management System, including FMIS:

- The Financial Management System's Security Plan – This plan would include the responsibilities of, or procedures implemented by, RRB staff for the controls that are specific to the two component applications (PAR and FMIS). This document would only have the detailed control information for the controls within the RRB's Financial Management System's boundaries. For the controls that are inherited or the portions of controls that are shared, this document would only refer to the other documents that have responsibilities for those controls or portions of controls. This document should be updated annually.
- The Agency Enterprise General Information Support System's Security Plan – This plan would reflect the controls that are inherited by the Financial Management System from the RRB's general support system. This document should be updated annually.
- The contractor's Information-as-a-Service Cloud System Security Plan – This plan is prepared by the contractor and reflects the controls implemented by the contractor for the infrastructure on which the FMIS application resides. This document is available through the General Services Administration's Federal Risk and Authorization Management Program (FedRAMP) website.
- The FMIS Application System Security Plan – This plan would include the responsibilities of, or procedures implemented by, the contractor's various support teams for controls that are specific to the FMIS application. The preparation of this SSP is currently not one of the procured services in the RRB's contract, so a contract modification would be required. This document should be updated annually.

The RRB has an increased risk of security exposures and control gaps when security documents are inaccurate or not updated timely to reflect the current process. By not reviewing and ensuring that the FMIS SSP accurately describes the security controls in place, there is a risk that the authorizing official will inappropriately consider the system to be within acceptable risk measures established by the agency.

Recommendations

4. The Bureau of Fiscal Operations should ensure that the control language within the Financial Management Integrated System Security Plan contains accurate and complete control information and includes all required controls from NIST SP 800-53, Revision 4.

5. The Bureau of Fiscal Operations should request a contract modification to include the preparation and annual update of the Financial Management Integrated System Security Plan as part of the procured services and deliverables.

Management's Response

The BFO partially concurs with recommendations 4 and 5. They consider the Financial Management System Security Plan as the primary vehicle for control language and information for the Financial Management System, leveraging control language and information from the Agency Enterprise General Information Support System's Security Plan, the contractor's cloud security plan required for FedRAMP certification, and the contractor's FMIS Application System Security Plan. The BFO will not contract for an annual update of the FMIS SSP, but will consult with the contractor on any update that may be indicated from continuous monitoring of the Financial Management System.

OIG's Comments on Management's Response

The OIG agrees with this alternative approach to ensuring accurate and complete control information exists for FMIS.

Inaccurate Audit and Accountability Procedures for Audit Records and Logs

The RRB's Audit and Accountability Processes and Procedures document does not reflect the current process for the review of audit records and logs, and is inconsistent with the RRB's Audit and Accountability Policy.

The section of the procedure document that relates to audit review, analysis, and reporting incorrectly states that audit records are reviewed annually when they actually are reviewed daily. In addition, the section for auditable events incorrectly states that audit records are reviewed annually, when it is actually the listing of auditable events that is reviewed annually.

NIST SP 800-53, Revision 4, requires that agencies review and update audit and accountability policies and procedures.

RRB management did not ensure that the correct language was documented in the Audit and Accountability Processes and Procedures. The procedures have also never been finalized. BIS is responsible for the agency's information system security policies and procedures. The Chief Security Officer informed us that BIS has been working with a limited staff, which has caused some tasks such as reviewing, updating, and finalizing specific policies and procedures to be delayed. An additional employee is expected to begin work by the end of fiscal year 2014.

The inaccurate Audit and Accountability Processes and Procedures document can result in an untimely review of the audit records and audit logs. There is an increased risk of security exposure and gaps in controls when policies and procedures are inconsistent or are not updated timely.

Recommendations

6. The Bureau of Information Services should review the RRB's information security processes and procedures for audit and accountability to ensure they properly reflect the current practices.

7. The Bureau of Information Services should ensure the RRB's policies and procedures are finalized and periodically reviewed and updated for accuracy.

Management's Response

The BIS concurs with recommendations 6 and 7. For recommendation 6 the Chief Security Officer will review the current processes and procedures for audit and accountability and ensure they properly reflect the current practices that are in place at the RRB. For recommendation 7, the Chief Security Officer is in the process of performing a review of all the RRB information security policies and procedures in IRM-18 and will have the review completed in fiscal year 2015. After the review has been completed, he will make certain that all of the policies and procedures have been finalized as directed.

Anticipated Migration of Program Accounts Receivable Application

During the course of our audit, we were advised that the RRB is planning to migrate the PAR component application of the Financial Management System to a system that fully integrates with FMIS. Funding for this project has been requested in the Congressional Justification of Budget Estimates for fiscal year 2015, and the RRB expects to begin preparing a Statement of Work in the near future.

The OIG has recently performed audits on the adequacy of the interface application controls and selected business process controls in FMIS, and reported similar deficiencies as noted in this report.[5] Specifically, we reported:

- the FMIS SSP did not adequately describe the interfaces and omitted information about applications and systems that interconnect with FMIS;
- policies and procedures were not clearly documented or maintained for FMIS transaction processing;
- selected business process controls for the preparation and approval of accounting transactions were not operating and effective because only partial or no supporting documentation was available;

[5] *Audit of the Adequacy of Interface Application Controls in the Financial Management Integrated System,* Report No. 14-11, August 14, 2014.
Audit of the Business Process Controls in the Financial Management Integrated System, Report No. 14-10, August 1, 2014.

- FMIS transactions had been modified by the Financial Systems Manager contrary to BFO policy; and
- FMIS security profiles were not always appropriate.

Lessons learned from the migration of FMIS can be effectively applied to reduce the risk of similar deficiencies when the RRB migrates to PAR.

Recommendation

8. The Bureau of Fiscal Operations should consider and apply related OIG recommendations and lessons learned from the FMIS migration when planning for, and migrating to, the fully-integrated PAR application.

Management's Response

The BFO concurs with recommendation 8. They will provide the PAR migration team and Contracting Officer's Representative with copies of the OIG findings and recommendations in this report and the OIG's audits on the adequacy of the interface application controls and selected business process controls in FMIS, as well as other lessons learned documentation from the FMIS migration.

UNITED STATES GOVERNMENT

MEMORANDUM

FORM G-115f (1-92)
RAILROAD RETIREMENT BOARD

September 18, 2014

TO : Heather J. Dunahoo
Assistant Inspector General for Audit

FROM : George V. Govan
Chief Financial Officer

George Govan

SUBJECT: Draft Report - Audit of the Data Management Application Controls and Selected General Controls in the Financial Management Integrated System

This is in response to your request for comments on the above draft report. Following are my comments on the recommendation addressed to the Bureau of Fiscal Operations (BFO).

The Bureau of Fiscal Operations should:

1. ***Ensure the BFO FMIS administrator acquires the expertise to implement access or changes in access without contractor assistance.***

   We concur. The FMIS administrator has acquired the expertise to make routine implementations and changes of access with the current security configuration supplied by CGI which comprises 180 different roles and over 4,000 security categories. The FMIS administrator will continue to make these routine implementations and changes as required by RRB clients but will continue to rely on support from the FMIS helpdesk for assistance in any modifications to the current configuration. Any change to the FMIS security configuration will be authorized by the FMIS administrator. As the legacy PAR system is migrated to FMIS, additional administration staff will be trained to implement and change access to FMIS.

   Target Completion Date: Implemented

2. ***Implement system-specific procedures for obtaining access to FMIS.***

   We concur and will follow a two phase approach;
   a. With the assistance of the Information Resources Management Center section of BIS, Security access forms tailored to the business requirements

of RRB organizations will be developed along with instructions and made accessible through the Boardwalk page of the RRB intranet.

b. Following the development of the forms and instructions, procedures for obtaining access to FMIS will be published and linked to IRM -18.

Target Completion Date: March 31, 2015

4. ***Ensure that the control language within the Financial Management Integrated System Security Plan contains accurate and complete control information and includes all required controls from NIST SP 800-53, Revision 4.***

See response for audit recommendation #5. Response is applicable to this recommendation.

5. ***Request a contract modification to include the preparation and annual update of the Financial Management Integrated System Security Plan as part of the procured services and deliverables.***

We partially concur with Recommendations 4 and 5. We regard the Financial Management (FM) SSP as the primary vehicle for control language and information for the FM major application which currently includes a *subsystem* – Program Accounts Receivable (PAR) system, and a *dynamic subsystem* – FMIS which employs a cloud computing architecture. This plan leverages control language and information from AEGIS, the contractor's cloud security plan which is required for FedRAMP certification and the contractor's FMIS Application SSP. Gaps in the controls identified during continuous monitoring will be addressed by BFO, if system specific, and BIS, if AEGIS. Common control gaps will be addressed in conjunction with the Chief Security Officer and hybrid controls with BIS or CGI depending on the subsystem. BFO will not contract for an annual update of CGI's FMIS Application SSP but will consult with CGI on any update that may be indicated from continuous monitoring of the FM SSP.

The target date for reviewing and approving the Security Assessment Report (SAR), System Security Plan (SSP), and Plan of Action and Milestones (POA&M) from DSD Laboratories for the Financial Management Information System Fiscal Year 2014 Continuous Monitoring is January 31, 2015.

Target Completion Date: January 31, 2015

8. ***Consider and apply related OIG recommendations and lessons learned from FMIS migration when planning for, and migrating to, the fully-integrated PAR application.***

We concur. We will provide copies of the OIG findings and recommendations from the audits of Business Process Controls in FMIS, Data Management

Application Controls and Selected Controls in FMIS, and Adequacy of Interface Application Controls in FMIS available to the PAR migration team and COR as identified in the PAR migration team charter. We will also make available the lessons learned deliverable from the contractor (KPMG LLP) which supported migration from FFS to FMIS.

Target Completion Date: September 30, 2014

If there is any additional information you need, please advise me.

cc: Tom McCarthy, Chief of TADS
Kris Garmager, Financial Systems Manager
Mike Zulevic, IT Specialist
Jean Hines, Financial Systems Specialist
Jerry Gilbert, Chief Security Officer
Susan Leszkowicz, Supervisory Auditor

United States Government
Memorandum

FORM G-115f (1-92)
Railroad Retirement Board

September 18 , 2014

TO: Heather J. Dunahoo
Assistant Inspector General for Audit

FROM: Ram Murthy
Chief Information Officer

SUBJECT: Draft Report – Audit of the Data Management Application controls and Selected General Controls in the Financial Management Integrated System.

This is in response to your request for comments on the above draft report. Following are my comments on the recommendation addressed to the Bureau of Information Services (BIS).

The Bureau of Information Services should:

3. The Bureau of Information Services should update the four general policy and procedure documents to include all systems requiring special access procedures.

BIS Response: We concur. The Chief Security Officer will update (1) Administrative Circular, Information Resource Management (IRM)-18, *Information Security Policy;* (2) Access Control Policy; (3) Access Control Processes and Procedures; and (4) Appendix A – RRB System Access Policy to include all systems requiring special access procedures.

Target Completion Date: March 31, 2015

6. The Bureau of Information Services should review the RRB's information security processes and procedures for audit and accountability to ensure they properly reflect the current practices.

BIS Response: We concur. The Chief Security Officer will review the current processes and procedures for audit and accountability and ensure they properly reflect the current practices that are in place at the RRB.

Target Completion Date: March 31, 2015

7. The Bureau of Information Services should ensure the RRB's policies and procedures are finalized and periodically reviewed and updated for accuracy.

BIS Response: We concur. The Chief Security Officer is in the process of performing a review of all the RRB information security policies and procedures in IRM-18 and will have the review completed in fiscal year 2015. After the review has been completed, he will make certain that all of the policy and procedures have been finalized as directed.

Target Completion Date: June 30, 2015

cc: Chief of Information Resources Management
Chief Security Officer