# FAA

Report QC2022018
January 31, 2022

## Quality Control Review of the Management Letter for the Federal Aviation Administration's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020

U.S. Department of Transportation
Office of Inspector General

Highlights

# Quality Control Review of the Management Letter for the Federal Aviation Administration's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020

*Required by the Chief Financial Officers Act of 1990*

**Federal Aviation Administration | QC2022018 | January 31, 2022**

## What We Looked At

This report presents the results of our quality control review (QCR) of the management letter that KPMG issued on its audit, under contract with us, of the Federal Aviation Administration's (FAA) consolidated financial statements for fiscal years 2021 and 2020. This management letter discusses internal control matters that KPMG was not required to include in its audit report.

## What We Found

Our QCR disclosed no instances in which KPMG did not comply, in all material respects, with U.S. generally accepted Government auditing standards.

## Our Recommendations

KPMG made six recommendations to FAA in its management letter. FAA concurred with all six recommendations.

# Contents

U. S. Department of Transportation
**Office of Inspector General**

# Memorandum

Date: January 31, 2022

Subject: INFORMATION: Quality Control Review of the Management Letter for the Federal Aviation Administration's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020 | Report No. QC2022018

From: Dormayne "Dory" Dillard-Christian
Acting Assistant Inspector General for Financial Audits

To: Federal Aviation Administrator

I am pleased to transmit the attached management letter related to the audit of the Federal Aviation Administration's (FAA) consolidated financial statements for fiscal years 2021 and 2020. KPMG LLP completed the audit under contract with us. The contract required that KPMG perform the audit in accordance with generally accepted Government auditing standards and the Office of Management and Budget's Bulletin 21-04, *Audit Requirements for Federal Financial Statements*. KPMG's auditor's report[1] included a clean (unmodified) opinion on FAA's financial statements.

KPMG also issued, and is responsible for, a management letter, dated November 30, 2021 (see attachment), identifying nine[2] internal control matters that require FAA management's attention. KPMG was not required to include these matters or the related recommendations in its auditor's report. We conducted a quality control review (QCR) of the management letter.

[1] See *Quality Control Review of the Independent Auditor's Report on the Federal Aviation Administration's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020* (OIG Report Number QC2022013), November 12, 2021.

[2] Three of these nine matters are control deficiencies related to DOT's internal controls and those of the Department's shared services center, the Enterprise Services Center (ESC) but also affect FAA's control environment. KPMG made recommendations to DOT and ESC to address these deficiencies but FAA is not required to take any corrective actions. We discuss these control deficiencies and recommendations in our following reports: *Quality Control Review on the Independent Auditors' Report on the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020* (OIG Report No. QC2022015), November 15, 2021, and *Quality Control Review of the Management Letter for the Department of Transportation's Audited Consolidated Financial Statements for Fiscal Years 2021 and 2020* (OIG Report No. QC2022017), January 31, 2022.

We appreciate the cooperation and assistance of FAA's representatives and KPMG. If you have any questions, please contact me at (202) 366-8543, or Ingrid Harris, Program Director, at (202) 450-7637.

cc: The Secretary
DOT Audit Liaison, M-1
FAA Audit Liaison, AAE-001

# Summary of Independent Auditor's Management Letter

In its management letter, KPMG reported the following deficiencies pertaining to FAA's information technology general and application controls and business process controls.

## Domain Password Controls

FAA's Default Domain Active Directory (AD) policy establishes password settings and account lock-out configurations for Windows servers within the FAA.gov domain. However, FAA did not have controls designed and implemented to ensure that database password requirements complied with its Information Security and Privacy Program and Policy (ISPP).

## Separation of Duties in the Time and Attendance System

FAA uses a time and attendance system owned by the Department of Transportation (DOT) and the Enterprise Services Center (ESC) manages the system's application, operating system, and database. However, ESC did not have controls to detect or prevent developers from migrating programmatic changes to the system's production web application environment which manages user functionality.

## Inventory System Configuration Management

Changes to FAA's inventory system application, database, and operating system are tracked using a ticketing system to document configuration management changes and patches. However, FAA did not have controls designed and implemented to ensure that changes to the inventory system application, database, and operating system were tested, documented, and approved prior to migration into production, as FAA's ISPP requires.

## Domain Account Lockout Threshold

FAA's Default Domain AD policy establishes password settings and account lockout configurations for Windows servers within the FAA.gov domain. However, FAA did not have controls in place and operating effectively over the policy to ensure compliance with FAA's ISPP. The Default Domain AD Policy was inappropriately configured to lock accounts after a higher number of failed login attempts than the number of failed attempts the Agency's ISPP allows.

## Controls Over the Completeness of the Legal Letter and Supporting Contingent Liability Report

FAA is routinely the subject of litigation that may require accrual and/or disclosure in its annual financial statements. The Agency's Office of the Chief Counsel prepares a legal letter and supporting contingent liability report that include all material cases to support the recording and disclosure of contingent legal liabilities. However, controls were not operating effectively to ensure completeness of the legal letter and the supporting report.

## Access to Payroll Shared Services Center

FAA uses a shared services center to process personnel actions and payroll and benefit-related transactions. However, controls over user access to the shared services center were not operating effectively. Specifically, FAA did not timely disable access to the shared services center for two users who left the Agency during fiscal year 2021.

## Recommendations

To strengthen FAA's information system and business process controls, KPMG recommended that FAA management:

1. Configure the password length for Windows server accounts within the FAA.gov domain to comply with FAA policy and system requirements.

2. Design and implement formal detective controls to log and monitor developer activities in the time and attendance system production environment. All programmatic changes to the time and attendance

system production environment should be reviewed and reconciled from the logs to the approved change tickets.

3. Design and implement a process to ensure that inventory system application, database and operating system changes are tested, documented, and approved prior to migration into production in accordance with FAA policy; and update the change management ticketing system to capture required approvals and evidence of testing for inventory system application, database or operating system changes.

4. Configure the account lockout threshold for the Windows server accounts within the FAA.gov domain to comply with FAA policy and system requirements.

5. Update the control to investigate cases removed from the Legal Letter and Contingent Liability Report period over period prior to recording the legal liability.

6. Ensure that policies and procedures for revoking access to the shared services center for separated users include:

    a. Timely notifying shared services center managers of FAA employees that have separated from the agency to ensure that access is removed; and

    b. Enforcing the timeline for removal of separated employees from shared services center, by reviewing active user listings on a periodic basis to ensure that no separated employees still have access.

FAA concurred with KPMG's six recommendations and provided a detailed action plan to address the findings issued to it in the management letter. In accordance with DOT Order 8000.1C, the corrective actions taken in response to the findings are subject to follow up.

# Quality Control Review

We performed a QCR of KPMG's management letter and related documentation. Our review disclosed no instances in which KPMG did not comply, in all material respects, with generally accepted Government auditing standards.

# **Exhibit.** List of Acronyms

| | |
|---|---|
| AD | Active Directory |
| DOT | Department of Transportation |
| ESC | Enterprise Services Center |
| FAA | Federal Aviation Administration |
| ISPP | Information Security and Privacy Program and Policy |
| QCR | quality control review |

# **Attachment.** Independent Auditor's Management Letter

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

November 30, 2021

Administrator, Federal Aviation Administration
Inspector General, U.S. Department of Transportation
Washington, DC

Ladies and Gentlemen:

In planning and performing our audit of the consolidated financial statements of the U.S. Department of Transportation (DOT) Federal Aviation Administration (FAA) as of and for the year ended September 30, 2021, in accordance with auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 21-04, *Audit Requirements for Federal Financial Statements*, we considered the FAA's internal control over financial reporting (internal control) as a basis for designing audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the consolidated financial statements, but not for the purpose of expressing an opinion on the effectiveness of the FAA's internal control. Accordingly, we do not express an opinion on the effectiveness of the FAA's internal control.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control that might be material weaknesses and/or significant deficiencies and therefore, material weaknesses and/or significant deficiencies may exist that were not identified. In accordance with *Government Auditing Standards*, we issued our report dated November 9, 2021 on our consideration of the FAA's internal control over financial reporting in which we communicated certain deficiencies in internal control that we consider to a significant deficiency.

A deficiency in internal control exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. In addition to the significant deficiency noted above, we identified the following other deficiencies in internal control related to general information technology and application controls and business process controls that are summarized in Exhibit I for your consideration.

This purpose of this letter is solely to describe the deficiencies in internal control identified during our audit. Accordingly, this letter is not suitable for any other purpose.

Very truly yours,

KPMG LLP

## A. General Information Technology and Application Controls

### FAA Domain Password Controls (NFR DOT-2021-FAA-IT-02)

*Background/Condition*

The FAA Default Domain Active Directory (AD) policy establishes password settings and account lock-out configurations for Windows servers within the FAA.gov domain. Account management functions for AD accounts are managed by the Account Management Team within the Infrastructure & Operations Service, Office of Information and Technology (AIT).

Controls are not designed or implemented over the AD policy to ensure compliance with FAA Information Security and Privacy Program & Policy (ISPP).

*Recommendation*

We recommend FAA management configure the password length for Windows server accounts within the FAA.gov domain to comply with FAA policy and system requirements.

### Developers Can Migrate Program Changes to the time and attendance system Production Environment (NFR DOT-2021-FAA-IT-03)

*Background/Condition*

FAA utilizes a time and attendance system categorized as a DOT owned system. The FAA Enterprise Service Center (ESC) manages the time and attendance system application, operating system, and database. Windows is the operating system running the application environment.

Controls are not designed to prevent or detect developers from migrating programmatic changes to the time and attendance system production web application environment, which manages user functionality.

*Recommendation*

We recommend system management design and implement formal detective controls to log and monitor developer activities in the time and attendance system production environment. All programmatic changes to the time and attendance system production environment should be reviewed and reconciled from the logs to the approved change tickets.

### Inventory System Configuration Management Weaknesses Exist (NFR DOT-2021-FAA-IT-09)

*Background/Condition*

Changes made to the inventory system application, database, and operating system are tracked using a ticketing system to document configuration management changes and patches.

Controls are not designed and implemented to ensure that the inventory application, database and operating system changes are tested, documented, and approved prior to migration into production, as required by the FAA ISPP.

*Recommendation*

We recommend management design and implement a process to ensure that inventory system application, database and operating system changes are tested, documented, and approved prior to migration into production in accordance with FAA policy; and update the change management ticketing system to capture required approvals and evidence of testing for inventory system application, database or operating system changes.

**Domain Account Lockout Threshold (NFR DOT-2021-FAA-IT-16)**

*Background/Condition*

The FAA Default Domain AD policy establishes password settings and account lock-out configurations for Window servers within the FAA.gov domain. Account management functions for AD accounts are managed by the AD group within the Office of Information and Technology (AIT).

Controls are not implemented and operating effectively over the AD policy to ensure compliance with FAA ISPP requirements for account lockout threshold. Instead, the FAA Default Domain Policy was inappropriately configured to lock accounts after 5 failed logon attempts.

*Recommendation*

We recommend FAA management configure the account lockout threshold for the Windows server accounts within the FAA.gov domain to comply with FAA policy and system requirements.

**Semi-annual review of administrator access was incomplete (NFR ESC-2021-02)**

*Background/Condition*

The DOT ESC performs privileged access reviews at the operating system level on a semi-annual basis. A script is executed on each server to obtain the list of local accounts with privileged access.

Controls over the semi-annual review of privileged operating system users were not operating effectively. The ESC management did not complete its review according to policy. Specifically, two of the operating system servers were not included in the semi-annual server administrator access review. Therefore, ESC management did not initially review, reauthorize, or remove the administrator accounts defined to these two severs. After been notified of this condition, ESC management retroactively completed the access reviews.

*Recommendation*

We recommend ESC management correct the ESC server inventory list to ensure that all production servers are correctly categorized and implement a quality assurance process to confirm that during the semi-annual review process, all servers and systems were included.

## B. Business Process Controls

### Weaknesses in Controls Over the Completeness of the Legal Letter (NFR FAA-2021-01)

*Background/Condition*

FAA is routinely the subject of litigation that may require accrual and/or disclosure in the annual financial statements. The Office of the Chief Counsel prepares a Legal Letter and supporting Contingent Liability Report to include all material cases to support the recording and disclosure of contingent legal liabilities.

Controls are not operating effectively to ensure that the completeness of the legal letter and the supporting Contingent Liability Report. Specifically, two open cases above the legal materiality was excluded from the Contingent Liability Reports, and one open case below the legal letter materiality was excluded from the Legal Letter and Contingent Liability report.

*Recommendation*

We recommend FAA update their control to investigate cases removed from the Legal Letter and Contingent Liability Report period over period prior to recording the legal liability.

### Access to Payroll Shared Service Center for FAA Separated Employees Not Revoked (NFR FAA-2021-02)

*Background/Condition*

FAA uses a shared service center to process personnel actions and payroll and benefit-related transactions. Controls over shared service center user access are not operating effectively. Specifically, FAA did not disable access to the shared service center timely for two (2) users who separated from FAA during FY 2021.

*Recommendation*

We recommend FAA management ensure that policies and procedures for revoking access to the shared service center for separated users includes:

- Timely notifying shared service center managers of FAA employees that have separated from the agency to ensure that access is removed.
- Enforcing the timeline for removal of separated employees from shared service center, by reviewing active user listings on a periodic basis to ensure that no separated employees still have access.

### Weakness in Controls Over Management Review and Approval of Journal Entries (NFR DOT-2021-02)

*Background/Condition*

FAA's manual journal entry process consists of two separate control environments, the Headquarters (HQ) and the ESC. ESC policy requires that all entries be reviewed by an appropriate member of the ESC accounting department within four business days of posting, to ensure that the entry is appropriate. Further, this review includes ensuring the entry is complete, accurate, and supported by adequate documentation.

Controls are not operating effectively to ensure that manual journal entries posted by the ESC are complete and accurate. Specifically, we identified one journal entry that did not reflect the intended financial statement impact stated in the supporting documentation.

*Recommendation*

We recommend the ESC update procedures surrounding management's review of journal entries at ESC to ensure that journal entries are reviewed at an appropriate level of precision to determine that all posted manual entries are complete, accurate, and adequately supported by documentation.

**DOT Monitoring of Service Organization Report – Payroll Shared Service Center (NFR DOT-2021-03)**

*Background/Condition*

DOT uses a shared service center to process personnel actions and payroll and benefit-related transactions. The shared service center receives an annual SSAE 18 SOC 1 Type 2 report that specifies complementary client controls that must be implemented and operating effectively to support the internal controls in place at the shared service center.

Controls over the review of the SOC-1 report are not operating effectively. Specifically, management did not appropriately document their considerations over the results of the service organization report, and the potential impact of findings in the SOC-1 report on its payroll process during FY 2021.

*Recommendation*

We recommend management implement policies and procedures to strengthen their process to assess applicable third-party service organization reports to include:

- Evaluating and documenting results of the SOC-1 report and related findings to appropriately assess their impact on the entity; and
- Completing a formal documented review of the SOC-1 report assessment to ensure that documentation is sufficient and appropriate.

U.S. Department of Transportation
**Office of Inspector General**

# Fraud & Safety Hotline

*https://www.oig.dot.gov/hotline*
*hotline@oig.dot.gov*
*(800) 424-9071*

## OUR MISSION

OIG enhances DOT's programs and operations by conducting objective investigations and audits on behalf of the American public.

1200 New Jersey Ave SE
Washington, DC 20590
www.oig.dot.gov