EXIM
EXPORT-IMPORT BANK
OF THE UNITED STATES

Office of Inspector General
Export-Import Bank
of the United States

Fiscal Year 2018
Financial Statements Audit
Management Letter

December 17, 2018
OIG-AR-19-02

Information about specific vulnerabilities in IT systems has been redacted from the publicly released version of this report. The information withheld was compiled in connection with OIG law enforcement responsibilities and consists of information that, if released publicly, could lead to the circumvention of the law.

To: Inci Tonguch-Murray,
Acting Senior Vice President and Chief Financial Officer

Howard Spira,
Senior Vice President and Chief Information Officer

From: Jennifer Fain,
Acting Assistant Inspector General for Audits and Evaluations

Subject: Fiscal Year 2018 Financial Statement Audit - Management Letter
OIG-AR-19-02

Date: December 17, 2018

This memorandum transmits KPMG LLP's (KPMG) Management Letter on the Export-Import Bank's (EXIM Bank) financial statements for fiscal years ended September 30, 2018 and 2017. Under a contract monitored by this office, we engaged the independent public accounting firm of KPMG to perform an audit of EXIM Bank's financial statements. The contract required the audit to be performed in accordance with United States generally accepted government auditing standards and Office of Management and Budget Bulletin No. 19-01, Audit Requirements for Federal Financial Statements.

This report contains comments and recommendations related to internal control deficiencies and other matters. KPMG identified three deficiencies in EXIM Bank's internal control over financial reporting. The three internal control deficiencies noted in this report were not significant and therefore, the deficiencies were not required to be reported in the EXIM Bank's independent audit report. KPMG's observations and recommendations, and management's responses regarding such matters are presented in the Attachment.

KPMG is responsible for the attached management letter dated November 15, 2018, and the conclusions expressed in the letter. We do not express opinions on EXIM Bank's financial statements, internal control, or conclusions on compliance with laws and regulations.

We appreciate the cooperation and courtesies provided to KPMG and this office during the audit. If you have questions, please contact me, Jennifer Fain at (202) 565-3439 or Jennifer.Fain@exim.gov. You can obtain additional information about the Export-Import Bank Office of Inspector General and the Inspector General Act of 1978 at www.exim.gov/about/oig.

cc: Jeffrey Gerrish, Acting President and Chairman
James Cruse, Acting First Vice President and Vice Chair
Jeffrey Goettman, Executive Vice President and Chief Operating Officer
Kevin Turner, Senior Vice President and General Counsel
Margaux Matter, Senior Vice President and Chief of Staff
David Sena, Senior Vice President of Board Authorized Finance
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Nicole Valtos, Vice President and Deputy Chief Operating Officer
Maria Fleetwood, Vice President, Acquisition and Business Services Division
Patricia Wolf, Controller, Vice President Controller
Nathalie Herman, Vice President, Treasurer
Stacy Dawn, Chief Information Security Officer and Chief Privacy Office
Cristopolis Dieguez, Director, Internal Controls and Compliance
Parisa Salehi, Acting Inspector General, OIG
Erica Wardley, Deputy Assistant Inspector General for Audits and Evaluations, OIG
Armando Mieles, Partner, KPMG LLP

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

November 15, 2018

Office of Inspector General
Export-Import Bank of the United States
Washington, DC

Office of the Chief Financial Officer
Export-Import Bank of the United States
Washington, DC

Ladies and Gentlemen:

In planning and performing our audits of the financial statements of Export-Import Bank of the United States (EXIM Bank) as of and for the years ended September 30, 2018 and 2017, 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 in accordance with Office of Management and Budget (OMB) Bulletin No. 19-01, *Audit Requirements for Federal Financial Statements*, we considered EXIM Bank'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 financial statements, but not for the purpose of expressing an opinion on the effectiveness of EXIM Bank's internal control. Accordingly, we do not express an opinion on the effectiveness of EXIM Bank's internal control.

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. A material weakness is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected, on a timely basis. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control was for the limited purpose described in the first 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 15, 2018 on our consideration of EXIM Bank's internal control over financial reporting.

During our audit, we identified deficiencies in internal control, which are summarized in Exhibit I. EXIM Bank's responses to the findings identified in our audit are also included in Exhibit I. EXIM Bank's responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on the responses.

The 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

KPMG LLP is a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity.

Exhibit I

Export-Import Bank of the United States

Management Letter Comments

FY2018

IT-NFR-2018-01 Database Privileged Access

Condition

EXIM Bank management did not properly design control activities to limit user access to information technology systems through authorization control activities, (b) (4) Specifically, during our review of privileged access to (b) (4) we noted:

- (b) (4)
- (b) (4)
- An effective process for (b) (4) has not been fully implemented.
- A process has not been implemented to ensure that individuals (b) (4)

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government states:

- Principal 11.14, Design of Security Management, "Management designs control activities to limit user access to information technology through authorization control activities such as providing a unique user identification or token to authorized users. These control activities may restrict authorized users to the applications or functions commensurate with their assigned responsibilities, supporting an appropriate segregation of duties. Management designs other control activities to promptly update access rights when employees change job functions or leave the entity. Management also designs control activities for access rights when different information technology elements are connected to each other."

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*, control AC-2 states: "The organization:

a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b) Assigns account managers for information system accounts;

c) Establishes conditions for group and role membership;

d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e) Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g) Monitors the use of information system accounts;

h) Notifies account managers:

   1. When accounts are no longer required;
   2. When users are terminated or transferred; and
   3. When individual information system usage or need-to-know changes;

i) Authorizes access to the information system based on:

   1. A valid access authorization;
   2. Intended system usage; and
   3. Other attributes as required by the organization or associated missions/business functions;

j) Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group."

NIST Special Publication (SP) 800-53 Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*, control AC-6 states: "The organization: The information system audits the execution of privileged functions."

a) Specifically: "Misuse of privileged functions, either intentionally or unintentionally by authorized users, or by unauthorized external entities that have compromised information system accounts, is a serious and ongoing concern and can have significant adverse impacts on organizations. Auditing the use of privileged functions is one way to detect such misuse, and in doing so, help mitigate the risk from insider threats and the advanced persistent threat (APT)."

NIST Special Publication (SP) 800-53 Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*, control IA-2 states: "The information system implements multifactor authentication for local access to privileged accounts."

Cause

The Bank did not perform a thorough risk assessment over (b) (4) to their information technology systems and thus failed to identify all of the risks associated with (b) (4) , including the specific risks (b) (4) .

Effect

The risk exists that individuals may have (b) (4) that is not based on (b) (4) principles.

Also, the risk exists that unauthorized/inappropriate activity could occur (b) (7)(E)

Additionally, if a (b) (7)(E)

Recommendations

We recommend that EXIM Bank management:

1. Create (b) (4) accounts (b) (4) accounts.
2. Limit the privileges of the (b) (4) to the roles needed to perform (b) (4) functions and responsibilities.
3. (b) (4), (b) (7)(E)
4. (b) (7)(E), (b) (4)
5. Enhance the (b) (4) controls to ensure (b) (4), (b) (7)(E) are properly monitored, reviewed, and that reviews are documented and communicated to management.

Management's Response

EXIM Bank concurs with the factual accuracy of all Notice of Finding and Recommendation (NFR) conditions.

(b) (7)(E)

This should completely address this condition. (b) (4), (b) (7)(E)

EXIM is in discussions with (b) (4) To mitigate this risk, (b) (7)(E)

EXIM is in the process of implementing (b) (4) . To mitigate the risk (b) (4) , EXIM has instituted a manual (b) (4) check (b) (4)

.

OCIO has evaluated the circumstances related to these observations and is confident that no compromise of the financial statements has occurred as a result of the observed conditions. The systems have been available and the Bank is not aware of any compromise of the integrity of the Bank's Data. Compensating controls including but not limited to (b) (4) are in place to detect changes to financial data whether intentional or due to system error. The systems involved in this observation did not include the (b) (4) .

<u>IT-NFR-2018-02 OS Incompatible Duties</u>

Condition

EXIM Bank management did not properly design control activities to implement separation of duties or the concept of least privilege between (b) (4) Specifically, during our review of the segregation of duties for operating system users, we noted (b) (4) for the (b) (4) have full administrator access to the production environment.

Criteria

NIST Special Publication (SP) 800-53 Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*, control AC-5 states: "The organization:

a) Separates [Assignment: organization-defined duties of individuals];

b) Documents separation of duties of individuals; and

c) Defines information system access authorizations to support separation of duties.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security Controls and Assessment Procedures for Federal Information Systems and Organizations*, control AC-2 states: "The organization:

a) Identifies and selects the following types of information system accounts to support organizational missions/business functions: [Assignment: organization-defined information system account types];

b) Assigns account managers for information system accounts;

c) Establishes conditions for group and role membership;

d) Specifies authorized users of the information system, group and role membership, and access authorizations (i.e., privileges) and other attributes (as required) for each account;

e) Requires approvals by [Assignment: organization-defined personnel or roles] for requests to create information system accounts;

f) Creates, enables, modifies, disables, and removes information system accounts in accordance with [Assignment: organization-defined procedures or conditions];

g) Monitors the use of information system accounts;

h) Notifies account managers:

   4. When accounts are no longer required;

   5. When users are terminated or transferred; and

   6. When individual information system usage or need-to-know changes;

i) Authorizes access to the information system based on:

   4. A valid access authorization;

   5. Intended system usage; and

   6. Other attributes as required by the organization or associated missions/business functions;

j) Reviews accounts for compliance with account management requirements [Assignment: organization-defined frequency]; and

k) Establishes a process for reissuing shared/group account credentials (if deployed) when individuals are removed from the group."

(b) (7)(E)

Cause

EXIM Bank did not have updated policies and procedures in place to prevent or detect (b) (4)

Effect

Without implementing effective segregation of duties, the risk exists that incompatible duties can be performed that can impact the overall security, availability, or integrity of the data that is relevant to financial reporting.

Recommendations

We recommend that EXIM Bank management:

6. Implement policies to ensure that incompatible roles for all information systems are documented and procedures are implemented to ensure that those roles are appropriately segregated, particularly in regards to (b) (4)

Management's Response

EXIM Bank concurs with the factual accuracy of all NFR conditions.

(b) (4), (b) (7)(E)

(b) (4), (b) (7)(E)

(b) (7)(E)

(b) (7)(E)

This ensured that there was no compromise of financial data.

FSA-NFR-2018-01 Cash Flow Model Documentation

Condition

During our audit, we reviewed EXIM Bank's models, management processes, documentation, and controls related to the financial statement re-estimates, which affect the allowance for losses and liability for loan guarantees reported in the financial statements.

The Cash Flow (CF) model combines historical data, with the probability of default (PD), recovery rate assumptions, the output from the Garman Kohlhagen (GK) and Loss Rate Factor (LRF) models, as well as data from the Economist Intelligence Unit (EIU) country ranking data, to calculate future cash flows for each deal. These future cash flows, are then input into the format required by the Office Management and Budget (OMB) Credit Subsidy Calculator (CSC), a required present value discount tool for agencies with credit reform programs, to generate subsidy re-estimates in accordance with the *Federal Credit Reform Act* (FCRA). We noted the following matters relating to the CF model:

- The model documentation should be enhanced to complement Standard Operating Procedures and other existing documents to describe, conceptually, how the CF model should work, and to provide sufficient details for an independent party to evaluate whether the actual model implementation is consistent with the conceptual model design. In addition, management should provide more details on the qualitative considerations (i.e., in addition to the qualitative factors applied in the model), such as the effects of the Project Finance deals, supporting overall model results that are more conservative than historical performance.

- The LRF model calculates lifetime PDs, i.e., the estimated PDs over the entire term of each deal. As deals age and show performance, industry practice would suggest that the total PD over the remaining life of a deal should be different from the lifetime PD. In other words, a deal with a lifetime PD of 10 percent in year 1, should have a remaining PD smaller than 10 percent in year 6, because it has performed as scheduled for 5 years. In the prior year, we noted that the PD was constant over the life of the deal. In FY 2018, EXIM Bank implemented a partial change to remedy this matter. The current LRF model shows that at 7 years for long-term deals, or 5 years for medium-term deals, the remaining PD is calculated and is gradually reduced over the remaining term. The model documentation should be enhanced to sufficiently support EXIM Bank's assumption that utilizing the lifetime PD will not have a significant impact on the overall results of the model.

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government states:

- Principle 10.03, Appropriate Documentation of Transactions and Internal Control, "Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained."

FASAB Technical Release 6, Preparing Estimates for Direct Loan and Loan Guarantee Subsidies under the Federal Credit Reform Act – Amendments to Technical Release No. 3 Preparing and Auditing Direct Loan and Loan Guarantee Subsidies under the Federal Credit Reform Act, states the following:

- Paragraph 17, "Agencies must accumulate sufficient relevant and reliable data on which to base cash flow projections. It is important to note that agencies should prepare all estimates and re-estimates based upon the best available data at the time the estimates are made. Agencies should prepare and report re-estimates of the credit subsidies, in accordance with SFFAS No. 2, 18, and 19, to reflect the most recent data available as discussed in the re-estimate section of this technical release. The OMB Circular A-11 also provides guidance on re-estimating credit subsidies. Guidance on the types of supporting documentation that is acceptable is found in paragraphs 20-22 of this technical release."

- Paragraph 20, "Documentation must be provided to support the assumptions used by the agency in the subsidy calculations. This documentation will not only facilitate the agency's review of the assumptions, a key internal control, it will also facilitate the auditor's review. Documentation should be complete and stand on its own, i.e., a knowledgeable independent person could perform the same steps and replicate the same results with little or no outside explanation or assistance. If the documentation were from a source that would normally be destroyed, then copies should be maintained in the file for the purposes of reconstructing the estimate."

- Paragraph 24, "Document the agency's cash flow model(s) used, the rationale for selecting the specific methodologies, and the degree of calibration within the model(s). Also, document the sources of information, the logic flow, and the mechanics of the model(s) including the formulas and other mathematical functions. In addition, document the controls over the model(s) used by the agency in preparing cash flow worksheets. Further, document that the cash flow model(s) reflect the terms of the loan contracts and, in a loan guarantee program, the loan guarantee contracts. Additional details regarding internal control are discussed in the specific fund/program procedures and controls section of the technical release."

- Paragraph 40, "The cash flow estimation process, including all underlying assumptions, should be reviewed and approved at the appropriate level including revisions and updates to the original model."

Cause

The existing CF model and credit reform re-estimate process was not documented at a level of detail that would enable an independent reviewer to assess the reasonableness of the cash flow model, its assumptions, and relevant qualitative considerations.

Effect

The CF is an integral part of the financial reporting process because of it's use for re-estimate calculations in the most significant balances and estimates at EXIM Bank. Management re-estimates calculation using the aforementioned model relies on complex computations and qualitative considerations. As a result, if CF model is not sufficiently documented, it could inhibit proper review, transparency, and governance of the FCRA re-estimate process, which could lead to a misstatement of the financial statements.

Recommendations

With respect to the cash flow model, we recommend that EXIM Bank management:

7. Continue to enhance the model documentation to articulate how the cash flow model works and the rationale used in the models. The documentation should be at a sufficient level of detail to enable a reviewer to independently analyze the model.
8. Assess the need to further modify the cash flow model to adjust the lifetime PD assumption to account for the age and performance of each deal, or document the determination as to how such a model change would have an insignificant effect on the model results.
9. Document, in sufficient detail, additional qualitative considerations used by management to calculate re-estimates for financial statement reporting, that clearly bridges the gap between model historical performance and the resulting calculations. The documentation should include a quantification of the impact of these qualitative considerations on the outputs of the cash flow model.

Management's Response

EXIM Bank concurs with the factual accuracy of all NFR conditions.

In FY 2018, EXIM Bank has increased documentation of the credit loss factor and cash flow methodology. EXIM Bank has also further documented the standard operating procedures related to the credit loss factors and cash flow methodology. EXIM will continue to enhance documentation in FY 2019 to provide further details on qualitative considerations and qualitative factors.

EXIM Bank believes that its improvements this year related to the lifetime PD reflect reasonable reserve levels and will enhance documentation as recommended by KPMG. Finally, EXIM Bank is committed to continuous improvement and each year analyzes ways to improve its estimates through either additional data elements or additional techniques. EXIM Bank will continue this process in the coming year related to the lifetime PD assumptions.

FSA-NFR-2018-02 Interest Income

Condition

In our sample testing of interest income for FY 2018, we identified 1 of 12 sample transactions where interest income and the related subsidy amortization was appropriately recorded upon the original billing, but was not appropriately reversed upon the cancellation of the billing, causing an $18 million overstatement. This transaction related to a project finance deal that included capitalized interest.

Criteria

Government Accountability Office (GAO) Standards for Internal Control in the Federal Government states:

- Principle 10.02, Response to Objectives and Risks, "Management designs control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks."

- Principle 10.04, Design of Appropriate Types of Control Activities, “Control activities can be either preventive or detective. The main difference between preventive and detective control activities is the timing of a control activity within an entity’s operations. A preventive control activity prevents an entity from failing to achieve an objective or address a risk. A detective control activity discovers when an entity is not achieving an objective or addressing a risk before the entity’s operation has concluded and corrects the actions so that the entity achieves the objective or addresses the risk.”

Cause

Controls were not effective to ensure that all aspects of the original entry were reversed when adjustments were made to the project finance billings. We noted that the posting logic in the Financial Management System (FMS) was incorrectly configured for the reversal/cancellation of billings (“credit memos”) related to the reversal of the capitalized interest schedules, and a detective control was not in place to identify that the reversing entry posted did not reverse the entire accounting string associated with the original billing entry.

Effect

Interest income and subsidy amortization was overstated for this transaction by $18 million in FY 2018. EXIM Bank performed an analysis of all credit memos issued on project finance deals with a schedule for capitalized interest that were cancelled/reversed during the year and found an additional $12.7 million in overstatements of interest income and subsidy amortization for the period of October 1, 2017 through September 30, 2018, and posted a correcting entry for $30.7 million.

Recommendations

We recommend that EXIM Bank management:

10. Develop and implement a correction to the FMS posting logic for credit memo account transactions.
11. Develop and implement controls to review the completeness and accuracy of posted journal entries for reversing/correcting transactions.

Management’s Response

EXIM Bank concurs with the factual accuracy of all NFR conditions.

EXIM Bank has developed the posting logic correction and will deploy the update to the Financial Management System – Next Generation once testing is finalized. EXIM Bank will continue to enhance internal controls over the completeness and accuracy of posted journal entries for reversing/correcting transactions.

Office of Inspector General
Export-Import Bank *of the* United States
811 Vermont Avenue, NW
Washington, DC 20571
202-565-3908
http://www.exim.gov/about/oig