EXPORT-IMPORT BANK OF THE UNITED STATES

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

Fiscal Year 2017
Financial Statements Audit
Management Letter

February 26, 2018
OIG-AR-18-03

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
David Sena, Senior Vice President of Board Authorized Finance
Howard Spira, Senior Vice President and Chief Information Officer

From: Erica Wardley, Acting Assistant Inspector General for Audits

Subject: Fiscal Year 2017 Financial Statement Audit - Management Letter
OIG-AR-18-03

Date: February 26, 2018

This memorandum transmits KPMG LLP's (KPMG) Management Letter on the Export-Import Bank's (EXIM Bank) financial statements for fiscal year ended 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. 15-03, *Audit Requirements for Federal Financial Statements*.

This report contains comments and recommendations related to internal control deficiencies and other matters. KPMG identified eight deficiencies in EXIM Bank's internal control over financial reporting. The eight 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 February 16, 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 Erica Wardley, (202) 565-3963 or Erica.Wardley@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: Scott P. Schloegel, First Vice President and Vice Chairman of the Board (Acting)
Kevin Turner, Senior Vice President and General Counsel
Jeff Goettman, Executive Vice President and Chief Operating Officer
Jessie Law, Senior Vice President, Chief of Staff and
White House Liaison
Kenneth Tinsley, Senior Vice President and Chief Risk Officer
Patricia Wolf, Vice President Controller
Nathalie Herman, Vice President Treasurer
John Lowry, Director, Information Technology Security and Systems Assurance
Cristopolis Dieguez, Director, Internal Controls and Compliance
Armando Mieles, Partner, KPMG LLP

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

February 16, 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 audit of the financial statements of Export-Import Bank of the United States (EXIM Bank), as of and for the year ended September 30, 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 Office of Management and Budget (OMB) Bulletin No. 17-03, *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. During our audit, we noted certain matters involving deficiencies in internal control and other operational matters that are presented for your consideration. These comments and recommendations, all of which have been discussed with the appropriate members of management, are intended to improve internal control or result in other operational efficiencies and are summarized in Exhibit I. We would be pleased to discuss these comments and recommendations with you at any time.

In addition, we identified a deficiency in internal control that we consider to be a significant deficiency, and communicated it in writing to management and those charged with governance on December 13, 2017. That matter is not repeated in Exhibit I.

Our audit procedures are designed primarily to enable us to form an opinion on the financial statements, and therefore may not bring to light all weaknesses in policies or procedures that may exist. We aim, however, to use our knowledge of EXIM Bank's organization gained during our work to make comments and suggestions that we hope will be useful to you.

This communication is intended solely for the information and use of management and the Office of Inspector General, and is not intended to be and should not be used by anyone other than these specified parties.

Very truly yours,

KPMG LLP

Exhibit I

Export-Import Bank of the United States
Management Letter Comments
FY2017

Segregation of Duties: (b) (4)

Background

In FY 2016, a control deficiency was identified by the prior auditor surrounding segregation of duties controls within the Change Management (CM) process for the (b) (7)(E), (b) application. It was noted that certain users, based on their assigned roles, had access to both development and production environments with respect to migrating (b) (4) application changes.

Condition

During part of FY 2017 (October 2016 through April 2017), we noted that:

- Users of both the (b) (4) and (b) (4) groups had access to develop and migrate (b) (4) application changes to production. [Repeat from FY 2016]
- (b) (4) changes migrated to the production environment were not tracked and reviewed to ensure that improper changes were not deployed. [Repeat from FY 2016]

Additionally, during FY 2017 we noted the following:

- Two (2) users were granted access to the (b) (4) role to deploy (b) (4) reports into the production environment and were also members of (b) (4) group responsible for developing and testing reports. These users do not perform report development as part of their job responsibilities, and, therefore, were inappropriately granted access to the (b) (4) group.
- One (1) user was granted access to the (b) (4) role to deploy repository database (metadata) changes into the production environment and was also a member of the (b) (4) group responsible for developing and testing reports. This user does not perform report development as part of his job responsibilities, and, therefore, was inappropriately granted access to the (b) (4) .

Criteria

Federal Information System Controls Audit Manual (FISCAM) presents a methodology for performing Information System (IS) control audits of federal and other governmental entities in accordance with professional standards. FISCAM, which is consistent with the GAO/PCIE *Financial Audit Manual* (FAM), *NIST Special Publication* (SP) *800-53* and other NIST and OMB IS control-related policies and guidance, is organized to facilitate effective and efficient IS control audits.

National Institute of Standards and Technology (NIST) *Special Publication* (SP) *800-53 Rev. 4* (Recommended Security Controls for Federal Information Systems and Organizations)

- AC-2 – Account Management

Control: The organization:

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

J. Reviews accounts for compliance with account management requirements [Assignment: organization defined frequency];

- AC-5 – SEPARATION OF DUTIES

Control: The organization:

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

b. Documents separation of duties of individuals; and

c. Defines information system access authorization to support separation of duties.

- AC-6 – Least Privilege

Control: The organization employs the principle of least privilege, allowing only authorized accesses for users (or process acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

Cause

- Lack of segregation of duties is due to the Bank's small team of qualified individuals able to manage development responsibilities and production migration.
- No segregation of duties policies and procedures were established to ensure user privileges are appropriate given the user's role.
- A comprehensive review of individuals with access to the (b) (4) application and changes deployed into (b) (4) was not completed, to ensure the level of access is commensurate with job responsibilities and only appropriate changes were being deployed.

Effect

Segregation of duties risks within the (b) (4) application, which are not monitored through system mitigation or manual mitigating controls, increases the risk of unauthorized database table changes which feed information to the (b) (4) reports being deployed into production and available in the (b) (4) dashboard. If the (b) (4) dashboard reports are utilized as part of the financial reporting process, the reports could have undergone unauthorized changes, hence increasing the risk of material misstatements in the financial statements.

Recommendation

Acknowledging the Bank's small team of qualified individuals, we understand the segregation of duties challenges. Therefore, we recommend the Bank:

Recommendation 1 – FY 2017

Document and implement a process for the periodic review of changes migrated to production to ensure that unauthorized changes do not bypass the change management process.

Management's Response

EXIM Bank concurs with the finding and recommendation. IMT management implemented a process effective May 2017 (b) (7)(E)

(b) (7)(E)

There were 2 (b) (4) who were in the (b) (4) group which gave them access to development and also they were part of the CM group which enables them migrate code to production. One (b) (4) left the Bank in 6/20/2017. The second person was removed from (b) (4) group and added to (b) (4) group which gives read only access to the development environment. This access change was completed on 7/13/2017.

Vulnerability Management Processes Needs Improvement

Background

On July 17-18, 2017, KPMG performed a vulnerability assessment of EXIM in accordance with the FY 2017 EXIM Information Security Testing Authorization Letter (STAL) on the following systems:

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

Condition

We noted that the Office of the Chief Information Officer (OCIO) vulnerability management processes need improvement. Specifically, we reviewed:

1. The Vulnerability Management Program (VMP) policy, effective December 1, 2013, and noted that the (b) (7)(E)

   ,

   the:

   - VMP is not officially signed and approved;
   - Roles and responsibilities are not established;
   - Tools used for scanning applications, databases, and websites are not defined;
   - Scanning techniques (b) (7)(E)
   - (b) (7)(E)
   - Remediation timelines are not defined; and,
   - (b) (7)(E)

2. The Network Scanning Policy (NSP), effective December 1, 2013, noted that the (b) (7)(E)

specifically, the:

- NSP is not officially signed and approved;
- Roles and responsibilities are not established;
- Scanning techniques (b) (7)(E) and,
- (b) (7)(E)

In addition, we noted that controls are not adequately designed and implemented to ensure the (b) (4) are appropriately scanned and monitored for vulnerabilities. Specifically, the (b) (4) , (b) (7)(E) .

Criteria

- (b) (7)(E)

- NIST SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, System and Information Integrity, SI-2, states:

  Control: The organization:

  a. Identifies, reports, and corrects information system flaws;

  b. Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation;

  c. Installs security-relevant software and firmware updates within [*Assignment: organization-defined time period*] of the release of the updates; and

d. Incorporates flaw remediation into the organizational configuration management process.

- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision (Rev.) 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Configuration Management, Control CM-6, states:

  Control: The organization:

  a. Establishes and documents configuration settings for information technology products employed within the information system using [*Assignment: organization-defined security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements;

  b. Implements the configuration settings;

  c. Identifies, documents, and approves any deviations from established configuration settings for [*Assignment: organization-defined information system components*] based on [*Assignment: organization-defined operational requirements*]; and

  d. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.

Cause

Management did not properly define the process and (b) (7)(E) were implemented timely. Additionally, EXIM has not done its due diligence in testing for a different (b) (7)(E) .

Effect

A lack of timely implementation (b) (7)(E) compromising the confidentiality, integrity, and availability of the data residing on the information system. (b) (7)(E), (b) (4)

Recommendations

We recommend that the EXIM OCIO:

Recommendation 2 – FY 2017

Update and implement policies and procedures to ensure that the identified vulnerabilities are monitored and tracked for remediation.

a. Ensure the (b) (7)(E) .

b. Ensure that all systems are being (b) (7)(E)

Recommendation 3 – FY 2017

Address the existing vulnerabilities identified during our assessment consistent with NIST guidelines.

Recommendation 4 – FY 2017

Continue to improve its vulnerability management program to help ensure that operating systems and applications are properly configured, and timely updated on a routine basis throughout the EXIM Bank enterprise.

Management's Response

Management agrees with the core meaning and intention of this finding and recommendation. However, while the VMP and Network Scanning Policy were not signed, they were none-the-less approved and represented the then-current vulnerability management program. (b) (7)(E)

Examples of this are found in the POA&M tracking spreadsheet that was provided to KPMG. Finally, EXIM Bank verified its (b) (4) vulnerability scan reports and confirmed that (b) (4) were included in these scans. EXIM Bank will ensure the new VMP policy will enforce the use of (b) (7)(E) and address the other recommendations made by KPMG.

EXIM Bank management has confidence in the security posture of the Bank as it affects the Bank financials and financial information systems.

User Access Separation – Interim Finding

Background

In FY 2016, a control deficiency was identified by the prior auditor over timely removal of access of separated employees and contractors. Certain users retained access to the (b) (4) and in-scope financial applications upon separation.

Condition

During FY 2017, the following deficiencies were noted:

- One (1) user who was separated from the Bank retained an active (b) (4) account for (b) (7)(E) .
- One (1) separated user maintained access to the in-scope (b) (4) application.

Criteria

Federal Information System Controls Audit Manual (FISCAM) presents a methodology for performing Information System (IS) control audits of federal and other governmental entities in accordance with professional standards. FISCAM, which is consistent with the GAO/PCIE *Financial Audit Manual* (FAM), *NIST Special Publication* (SP) *800-53* and other NIST and OMB IS control-related policies and guidance, is organized to facilitate effective and efficient IS control audits.

National Institute of Standards and Technology (NIST) *Special Publication* (SP) *800-53 Rev. 4* (Recommended Security Controls for Federal Information Systems and Organizations)

- AC-2 Account Management

Control: The organization:

f. Creates, enables, modifies, disables, and removes information system accounts;

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;

Cause

- The user's (b) (4) account was not disabled in a timely manner after receiving the separation email notice.
- Oversight on the part of the administrators responsible for terminating the user's (b) (4) access due to an attachment being left off the (b) (4) Service Request ticket.

Effect

If access were to be exploited, unauthorized changes could have been made to the Bank's financial reporting systems.

Recommendations

We recommend the Bank:

Recommendation 5 – FY 2017

Enhance the current process requiring all (b) (4) service request tickets for access terminations to include attachments identifying each individual user to be deactivated.

Recommendation 6 – FY 2017

Enhance the current processes for off-boarding and periodic review of users with (b) (4) accounts to ensure that (b) (4) are disabled in a timely manner upon the user's separation from the Bank.

Management's Response

EXIM Bank agrees with the finding and recommendation. The impact of either instance on the Bank's financial systems are negligible as in neither case was access allowed that would have permitted either user to conduct any actions on the Bank's IT systems. In the first case, the user whose (b) (4) account remained open was prevented from accessing the network due to the absence of an (b) (4) , a (b) (4) , and a (b) (4) account – each of which is required to access and navigate the Bank network. This user could not have accessed any internal application to which the user had a user account. EXIM Bank's review of the applicable logs demonstrates that this user did not. In the second case, while the user (an intern) retained access to (b) (4) after separation from the Bank, this user had read-only permissions in (b) (4) and could not have modified any data in this system to threaten data integrity in (b) (4) . Finally, a log review of (b) (4) logs confirmed that this user did not access (b) (4) following separation. Going forward, an upcoming change in authentication (b) (7)(E), (b) (4) will enhance security of (b) (7)(E) at the Bank and eliminate the manual process of reviewing (b) (4) . Additionally, EXIM Bank will review the (b) (4) account review process' effectiveness. This will be completed by January 2018.

User Access Separation – Roll Forward Finding

Background

During FY 2017 roll forward testing, we noted that one contractor retained inappropriate access after leaving EXIM Bank.

Condition

KPMG noted one terminated contractor retained access to an (b) (7)(E) 64 days after leaving the Bank. Specifically, the contractor was terminated on August 9, 2017 and continued to have an active account at the time of testing on October 12, 2017.

Criteria

Federal Information System Controls Audit Manual (FISCAM) presents a methodology for performing Information System (IS) control audits of federal and other governmental entities in accordance with professional standards. FISCAM, which is consistent with the GAO/PCIE *Financial Audit Manual* (FAM), *NIST Special Publication* (SP) *800-53* and other NIST and OMB IS control-related policies and guidance, is organized to facilitate effective and efficient IS control audits.

National Institute of Standards and Technology (NIST) *Special Publication* (SP) *800-53 Rev. 4* (Recommended Security Controls for Federal Information Systems and Organizations)

- AC-2 Account Management

Control: The organization:

f. Creates, enables, modifies, disables, and removes information system accounts;

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;

KPMG noted the following in EXIM's Access Control Policy:

- 6.1.4 - Timely (b) (7)(E) modification of account accesses and privileges is required when a user's role changes.
- 6.2.9 - Individual identifiers and authenticators for the LAN and all applications must be immediately deactivated under the following conditions: (1) whenever notified by a user's authorizing official that the user no longer requires access; or (2) whenever notified by a proper authority (e.g., human resources, COTR) that the user's employment with the Bank has been terminated.

Cause

EXIM's termination processes do not ensure that all user accounts for terminated personnel are disabled across all applications and systems in a timely manner.

Effect

By not properly removing access for terminated users, there is an increased risk of unauthorized use, disclosure, or damage of EXIM resources.

Recommendations

We recommend the Bank:

Recommendation 7 – FY 2017

Modify the current termination process in order to ensure that all accounts are disabled within (b) (7)(E) of the employee/ contractor effectively being terminated from the bank.

Recommendation 8 – FY 2017

Enhance the current processes for off-boarding of users to ensure that the IT Help Desk and IT Infrastructure group are notified about removing access within a timely manner from employee/contractor separation.

Management's Response

While EXIM Bank agrees that the user account on the (b) (7)(E) should have been closed in a more timely manner and in the future they will endeavor to do so, the access controls for the Bank's IT systems worked as expected and no access to this account was permitted as evidenced by the (b) (7)(E)

The Bank's access controls are built with layers of security as other security controls in use at the Bank. The access control architecture for the Bank's IT systems are such that each of the following must be true in order for a privileged users to gain access to an IT system, namely: (b) (7)(E)

(b) (7)(E)

Background

In FY 2016, a control deficiency was identified by the prior auditor as a result of (b) (7)(E) history settings for two (b) (7)(E) that were not (b) (7)(E) in accordance with the Bank's Access Control Policy and IT Rules of Behavior Policy. Additionally, (b) (7)(E) were not in compliance with the (b) (7)(E) requirements established in the Bank's Access Control Policy and IT Rules of Behavior Policy.

Condition

In FY 2017, the Bank did not develop/enhance and implement (b) (7)(E) policies to include each application and infrastructure layer, (b) (7)(E) , and (b) (7)(E)

Criteria

Federal Information System Controls Audit Manual (FISCAM) presents a methodology for performing Information System (IS) control audits of federal and other governmental entities in accordance with professional standards. FISCAM, which is consistent with the GAO/PCIE *Financial Audit Manual* (FAM), *NIST Special Publication* (SP) *800-53* and other NIST and OMB IS control-related policies and guidance, is organized to facilitate effective and efficient IS control audits.

National Institute of Standards and Technology (NIST) *Special Publication* (SP) *800-53 Rev. 4* (Recommended Security Controls for Federal Information Systems and Organizations)

- IA-5 – Authenticator Management

Control: The organization manages information system authenticators by:

B. Establishing initial authenticator content for authenticators defined by the organization;

C. Ensuring that authenticators have sufficient strength of mechanism for their intended use;

E. Changing default content of authenticators prior to information system installation;

F. Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators;

G. Changing/refreshing authenticators [*Assignment: organization-defined time period by authenticator type*];

I. Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators.

Cause

(b) (7)(E) have not been documented for all applications and devices. According to management, this is due to the Bank's resource limitations and its prioritization of effort over other IT security related activities.

Effect

The lack of (b) (7)(E) / standards and implementation of these standards increases the risk a (b) (7)(E) may be guessed or obtained by an unauthorized individual and used to gain access to key financial reporting applications.

Recommendation

We recommend the Bank:

Recommendation 9 – FY 2017

Document/enhance and implement (b) (7)(E) and standards to include all operating systems, databases, applications, and network devices.

Management's Response

EXIM Bank agrees with the finding and recommendation. As of August 30, 2017, IMT staff closed an IT Security Program of Action and Milestones (POA&M) entry which was opened in response to the finding that resulted from the prior year 2016 FISCAM audit. IMT staff created and IMT management reviewed and approved (b) (7)(E) settings, procedures, and scripts for its (b) (7)(E), (b) (4)

(b) (7)(E), (b) (4) These documents are available for inspection to demonstrate closure of both last year's finding and this year's modified finding. This was closed on August 30, 2017.

Recordkeeping of Guaranteed Loan Credits

Background

Guaranteed credits are a significant portion of the Bank's portfolio, with approximately $46.6 billion guaranteed balance as of September 30, 2017. Prior to authorization and when guaranteed credits are amended, management has effective controls in place to ensure the transactions are properly approved, have followed the appropriate internal process, and the information is accurately captured in the Bank's records. For some of the guaranteed credits, it is not uncommon for the payment terms to be modified subsequent to the initial authorization of the guarantee and not trigger a formal transaction amendment. These modifications could impact the payment amortization schedule for the remaining life of the credit that is guaranteed, which affects the amount of the outstanding guarantee balance, which is used in developing the Guaranteed Loan Liability and guaranteed balance amounts/disclosures in the Bank's financial statements.

Condition

Based on our confirmation procedures, we identified various guaranteed credits for which repayment amortization schedules had changed. As a result, the outstanding guaranteed balance records for those guarantees were not accurate as of September 30, 2017.

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."
- Principle 13.04, "Management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Sources of data can be operational, financial, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring."

Cause

Management has designed and implemented effective controls to capture all relevant information for authorizations and change of terms, when they trigger a formal amendment. However, these processes and controls were not sufficiently designed and implemented to ensure that the repayment amortization schedules related to existing guaranteed credits are accurate and reflect the most current terms of the transactions when payment terms are modified without a formal transaction amendment.

Effect

The guaranteed credit balances are the most significant driver of the Guaranteed Loan Liability balance on the financial statements, and affect the accuracy of the guaranteed balance disclosures in the financial statement footnotes. If processes and controls surrounding future repayment term modifications are not enhanced, errors in the accounting for guarantee programs could result in misstatements to the financial statements. It should be noted, that our audit procedures demonstrated that the variances identified did not significantly affect the September 30, 2017 financial statements.

Recommendation

We recommend the Bank:

Recommendation 10 – FY 2017

Develop and implement procedures and internal controls over the guarantee portfolio balance monitoring process, to ensure the records related to each credit guaranteed are accurate and capture all relevant and current repayment amortization schedule of the transaction.

Management's Response

EXIM Bank concurs with the recommendation. EXIM Bank will enhance internal controls similar to controls on new authorizations and amendments to ensure outstanding balances for guaranteed credits are accurate and capture current repayment amortization schedules for the transactions.

Budget Cost Level (Credit Score Process) Documentation

Background

EXIM is backed by the full faith and credit of the United States and assumes credit and country risks that the private sector is unable or unwilling to accept. As part of the on-going monitoring of EXIM deals, or credits, management performs a credit review of each individual deal, throughout the year, to determine if changes to the original or previous score, commonly referred as Budget Cost Level (BCL) are needed.

The BCL score ranges from 1 (best possible score) to 11 (worst possible score). The BCL scores are also an important input in management's re-estimate calculations for financial statement reporting under the *Federal Credit Reform Act* (FCRA).

Condition

During our audit procedures related to the BCL rating process, we noted the following:

- The Transportation Portfolio Management Division (TPMD) Scorecard, the Asset Management Division (AMD) – Project Financing Scorecard, and the AMD – Corporate Scorecard, used to derive the BCL ratings for each credit, contain a number of judgmental qualitative inputs that impact the final BCL rating assigned. Improvements related to the documentation around the judgments made to assign the final BCL are needed in order to enable a reviewer to easily assess the reasonableness of the BCL score assigned.

- Management's BCL credit score review occurs throughout the year. However, we noted that management does not have detailed documentation, available for examination, to support the assessment that the BCL credit scores should not change from the date of the annual review to the financial statement date, or the date on which FCRA re-estimates are performed that use these BCL credit scores. In these cases, detailed documentation is needed to justify that the credit score determinations at an interim date remain relevant for use in of the re-estimate calculation that determines the Guaranteed Loan Liability and Allowance for Loan Losses. Based on discussions with management, we understand that update considerations are only documented for deals where a BCL change was assessed as needed between the interim and year-end date.

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."

Cause

Management has documentation over their BCL credit score process; however, is not sufficiently comprehensive to describe judgments around qualitative inputs and determinations impacting the BCL annual credit score. Additionally, while there is active credit monitoring performed by various divisions at EXIM, such monitoring is not consistently documented and readily available for examination to evidence that a BCL rating remains relevant as of the date that the financial statement reestimates are performed.

Effect

The current extent of documentation over the BCL credit score processes, determinations, and judgments could result in the assignment of a different BCL rating depending on the individual who is assigning the rating. Furthermore, if the active monitoring process is not sufficiently documented, it could limit management's ability to detect an incorrect BCL from being used in the re-estimate process, thus impacting the Guaranteed Loan Liability and Allowance for Loan Losses in the financial statements.

Recommendations

We recommend the Bank consider:

Recommendation 11 – FY 2017

Expanding the documentation of the BCL credit score determinations by requiring preparers and reviewers to describe rationale, judgments, and decisions related to qualitative inputs. The documentation should be at a sufficient level of detail to enable an independent reviewer to arrive at the same BCL determination and be readily available for examination.

Recommendation 12 – FY 2017

Formalizing a process to supplement the active monitoring of the portfolio by documenting an update for those deals where the annual BCL review was performed prior to the date that the FCRA re-estimates for financial statements are calculated. The documentation should be at a sufficient level of detail to enable an independent reviewer to understand the update procedures performed and conclusions reached, and be readily available for examination.

Management's Response

EXIM Bank concurs with the recommendations. EXIM Bank will enhance the documentation of individual "qualitative" inputs (that roll up into the final overall BCL rating) to enable a technical independent reviewer to more easily assess the reasonableness of the BCL assignment. EXIM Bank will also document roll forward procedures for BCL ratings that take place between the date the annual BCL review is completed and the date the FCRA reestimates are calculated.

Controls over Financial Statement Preparation and Reporting

Background

Financial reporting relates to the preparation of financial information to be included in the financial statements and related disclosures, and includes the procedures used to enter transaction totals into the general ledger, procedures related to the selection and application of accounting policies, and management's oversight of the process.

Condition

Controls to timely identify and report budgetary and proprietary account balances in EXIM Bank's annual financial statements in accordance with generally accepted account principles (GAAP) for Federal entities, specifically the Federal Accounting Standards Advisory Board (FASAB) Standards need improvement.

In FY 2017, management designed and implemented additional processes and controls over financial reporting. As part of this process, errors were identified relating to an omission of the financial statement caption Distributed Offsetting Receipts that should be reported on the Statement of Budgetary Resources and the incorrect presentation of an Other Financing Source reported as a Budgetary Financing Source on the Statement of Changes in Net Position. These errors were corrected for the FY 2017 financial statements to align with GAAP, but also existed in the prior year.

Criteria

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

- Principle 10.02, "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. As part of the control environment component, management defines responsibilities, assigns them to key roles, and delegates authority to achieve the entity's objectives."

- Principle 13.04, "Management obtains relevant data from reliable internal and external sources in a timely manner based on the identified information requirements. Relevant data have a logical connection with, or bearing upon, the identified information requirements. Reliable internal and external sources provide data that are reasonably free from error and bias and faithfully represent what they purport to represent. Management evaluates both internal and external sources of data for reliability. Sources of data can be operational, financial, or compliance related. Management obtains data on a timely basis so that they can be used for effective monitoring."

Statement of Federal Financial Accounting Standards No. 7, *Accounting for Revenue and Other Financing Sources and Concepts for Reconciling Budgetary and Financial Accounting,* states:

- "Other Financing Sources: Inflows of resources that increase net position of a reporting entity but that are not revenues or gains. Borrowing is not included as other financing sources, since it does not increase the net resources of the reporting entities."

- "78. Recognition and measurement of budgetary resources should be based on budget concepts and definitions contained in OMB Circulars No. A-11 and No. A-34."

Office of Management and Budget (OMB) Circular No. A-11, *Preparation, Submission, and Execution of the Budget,* Section 11, *Statement of Budgetary Resources,* states:

- "While the above entries include tables to prepare the SF 133, Report on Budget Execution and Budgetary Resources, the Statement of Budgetary Resources is a financial statement that is based on the SF 133 format but only includes the following lines. Refer to OMB Circular No. A-136 for guidance on preparing financial statements. The descriptions below identify the relationships of the lines of the SBR with the lines on the SF 133 and Schedule P."

- "Line 4200 – Distributed offsetting receipts: Collections that are offset against gross outlays and budget authority but are not authorized to be credited to expenditure accounts are credited to receipts accounts and are offset at the agency level."

- "Line 4210 – Agency outlays, net: Sum of Outlays, net minus Distributed offsetting receipts"

OMB Circular No. A-136, *Financial Reporting Requirements,* Section II.4.5, *Statement of Changes in Net Position*, Section II.4.5.6, *Other Financing Sources*, states:

- "This section displays financing sources and nonexchange revenues that are not budgetary resources."
- "Other. This includes financing sources that do not represent budgetary resources and are not otherwise classified above."

Cause

During FY 2016, management's financial reporting processes and controls were not sufficient to identify the errors in disclosures cited above. Management has designed and is in the process of implementing management/supervisory review controls over the financial statement preparation and reporting process to ensure that the financial statements and related disclosures are complete and reported properly, in accordance with GAAP and the general guidance for Government Corporations outlined in OMB Circular A-136, *Financial Reporting Requirements*.

Effect

Ineffective internal controls in the financial statement preparation and reporting process increases the risk that the financial statements and related disclosures may be incomplete or inaccurate.

Recommendation

We recommend the Bank:

Recommendation 13 – FY 2017

Continue to develop and implement internal controls over the preparation and review the annual financial statements and related disclosures, such as developing/using a financial reporting checklist to mitigate the risk of non-compliance with GAAP and, where applicable, the general guidance for Government Corporations outlined in OMB Circular A-136, *Financial Reporting Requirements*.

Management's Response

EXIM Bank concurs with the recommendations. EXIM Bank will continue to enhance internal controls over the preparation and review of the annual financial statements and related disclosures and will execute such controls earlier in the financial reporting process.

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