OFFICE OF INSPECTOR GENERAL
EXPORT-IMPORT BANK
***of the* UNITED STATES**

Independent Audit on the Export-Import Bank's Planning and Implementation of the Financial Management System-Next Generation (FMS-NG)

March 31, 2015
OIG-AR-15-05

EXPORT-IMPORT BANK
***of the* UNITED STATES**
INSPECTOR GENERAL

To: David Sena
Chief Financial Officer

Howard Spira
Chief Information Officer

From: Terry Settle TLS
Assistant Inspector General for Audits

Subject: Independent Audit on the Export-Import Bank's Planning and Implementation of the Financial Management System-Next Generation (FMS-NG)

Date: March 31, 2015

This memorandum transmits Cotton & Company LLP's audit report on the Export-Import Bank's Planning and Implementation of the Financial Management System-Next Generation (FMS-NG). Under a contract monitored by this office, we engaged the independent public accounting firm of Cotton & Company to perform the audit. The objective of the audit was to determine whether Ex-Im Bank's planning and implementation of FMS-NG was adequate and effective.

Cotton & Company determined that there were no significant issues or major risks that would prevent the implementation of FMS-NG. The Bank committed senior level personnel to significant components of the implementation effort. In addition, the Bank had adequate processes for documenting and tracking changes to the system and ensuring appropriate security for system interfaces. However, we found that improvements could be made with the planning and documentation of the implementation of FMS-NG. The report contains seven recommendations and management concurred with all recommendations. We consider management's proposed actions to be responsive and the recommendations will be closed upon completion and verification of the proposed actions.

We appreciate the cooperation and courtesies provided to Cotton & Company and this office during the audit. If you have questions, please contact me at (202) 565-3498 or terry.settle@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/oig.

cc: Fred Hochberg, Chairman and President
Angela Freyre, General Counsel
C.J. Hall, Executive Vice President and Chief Risk Officer
Audit Committee
Michael Cushing, Senior Vice President and Chief Operating Officer
John Lowry, Director, Information Technology Security and Systems Assurance
Inci Tonguch-Murray, Deputy Chief Financial Officer
Cristopolis Dieguez, Business Compliance Analyst
George Bills, Partner, Cotton & Company LLP

Cotton & Company LLP
635 Slaters Lane
4th Floor
Alexandria, VA 22314

P: 703.836.6701
F: 703.836.0941
www.cottoncpa.com

March 31, 2015

Terry Settle
Assistant Inspector General for Audits
Export-Import Bank
811 Vermont Avenue, NW
Washington, DC 20571

Subject: Independent Auditor's Report on the Export-Import Bank's Planning and Implementation of the Financial Management System – Next Generation (FMS-NG)

Dear Ms. Settle:

We are pleased to submit this report in support of audit services provided to determine whether the Export-Import Bank of the United States (Ex-Im Bank or the Bank) adequately planned for and implemented its new financial system. Cotton & Company LLP conducted an independent audit of Ex-Im Bank's Financial Management System – Next Generation (FMS-NG) planning and implementation process, from identification of requirements and selection of the new financial system to user acceptance testing, training of users, and placement of the financial system into production. Cotton & Company performed the work from September 2014 through January 2015.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as amended, promulgated by the Comptroller General of the United States. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence that provides a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence we obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Please feel free to contact me with any questions.

Sincerely,

COTTON & COMPANY LLP

George E. Bills, CPA, CISSP, CISA, CIPP
Partner

The Export-Import Bank of the United States (Ex-Im Bank) is the official export-credit agency of the United States. Ex-Im Bank is an independent, self-sustaining executive agency and a wholly-owned U.S. government corporation. Ex-Im Bank's mission is to support jobs in the United States by facilitating the export of U.S. goods and services. Ex-Im Bank provides competitive export financing and ensures a level playing field for U.S. exports in the global marketplace.

The Office of Inspector General, an independent office within Ex-Im Bank, was statutorily created in 2002 and organized in 2007. The mission of the Ex-Im Bank Office of Inspector General is to conduct and supervise audits, investigations, inspections, and evaluations related to agency programs and operations; provide leadership and coordination as well as recommend policies that will promote economy, efficiency, and effectiveness in such programs and operations; and prevent and detect fraud, waste, abuse, and mismanagement.

ACRONYMS

CFO	Chief Financial Officer
CIO	Chief Information Officer
F&AS	Financial and Administrative System
FMS-NG	Financial Management System – Next Generation
FY	Fiscal Year
GL	General Ledger
GSS	General Support System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
SA&A	Security Assessment & Authorization
SDLC	System Development Life Cycle
SP	Special Publications

Executive Summary

March 31, 2015

Independent Audit of Ex-Im Bank's Implementation of FMS-NG

OIG-AR-15-05

Why We Contracted for This Audit

In fiscal year (FY) 2012, the Export-Import Bank of the United States (Ex-Im Bank or the Bank) Offices of the Chief Financial Officer (CFO) and the Chief Information Officer (CIO) initiated a project to replace Ex-Im Bank's legacy financial and administrative information technology systems with the Financial Management System – Next Generation (FMS-NG). FMS-NG is a commercial-off-the-shelf (COTS) Financial Systems Integration Office (FSIO) and credit-reform-compliant system comprised of Oracle Federal Financials and Oracle Loans. The Office of Inspector General contracted with Cotton & Company LLP to conduct a performance audit of Ex-Im Bank's implementation of FMS-NG.

What We Recommended

We made seven recommendations for Ex-Im Bank to (1) appropriately plan, prepare, and maintain sufficient and appropriate documentation for data-conversion activities, (2) gather and save key evidence of FMS-NG data-conversion activities, such as detailed tie-outs of converted data, data maps and crosswalks used, approvals, and logs of errors and their resolution, (3) centrally organize and maintain all planning, converting, testing and implementation documentation so that it is readily available, (4) document formal account management procedures for the request, approval, creation, review, and removal of FMS-NG accounts, (5) develop and implement an access request form to facilitate the account management process, (6) develop and implement separation-of-duties requirements for FMS-NG administrators, and (7) for current and future system implementations, develop and document contingencies for essential functions in the event that they do not operate effectively post-implementation. Management concurred with all seven recommendations.

What Cotton & Company LLP Found

The objective of this audit was to determine whether Ex-Im Bank's planning and implementation of FMS-NG was adequate and effective. During our review, we did not identify any significant issues or major risks that would prevent the implementation of FMS-NG. We noted that the Bank committed senior level personnel to significant components of the implementation effort. Furthermore, we noted that the Bank had adequate processes for documenting and tracking changes to the system and ensuring appropriate security for system interfaces. However, we found that improvements could be made with the planning and documentation of the implementation of FMS-NG.

Specifically, Ex-Im Bank did not develop and maintain comprehensive project plans and supporting documentation to ensure that the migration to FMS-NG fully adhered to established plans and that business operations could continue without significant complications. While the Bank developed high-level project plans, the plans did not always include the associated procedures for carrying out the plans. Furthermore, the Bank did not continuously update its plans to ensure they were accurate and reflected required changes. Overall, it was very difficult for the audit team to identify and follow the planned and performed procedures. Documentation was not organized and readily available and we found that the procedures that were performed did not always tie back to the planning documents. While we were able to gain an understanding of the data conversion planning and validation efforts through the high-level planning documentation, interviews, walkthroughs, and the validation results provided by the Bank, we found that the Bank:

- Did not sufficiently plan and document the data-conversion process.
- Did not perform adequate security assessment and authorization (SA&A) activities for FMS-NG access controls.
- Did not develop a contingency plan in the event the system was a "no-go" on the production date or had errors during the implementation that prevented it from operating effectively.

The above weaknesses represent increased risks to the Bank's overall ability to promptly identify the root cause of errors and defects in the data; process routine transactions; understand security vulnerabilities and internal control weaknesses in the system; and identify and address issues, constraints or errors in the system. As a result, Ex-Im Bank's normal operations could be delayed or impaired. For example, we identified that purchase card payments and travel reimbursements were not paid in a timely manner and Ex-Im Bank financial reports were delayed.

These areas require increased attention as system implementation continues and during future audits.

For additional information, contact the Office of the Inspector General at (202) 565-3908 or visit www.exim.gov/oig.

TABLE OF CONTENTS

INTRODUCTION

Objective

This report presents the results of Cotton & Company LLP's audit of the Export-Import Bank of the United States (Ex-Im Bank or the Bank)'s planning and implementation of the Financial Management System – Next Generation (FMS-NG). The objective of this performance audit was to:

1. Identify and assess procedures used by Ex-Im Bank to ensure that data interfaces would completely and accurately transfer data from the legacy systems to FMS-NG on production date.
2. Identify and assess procedures used by Ex-Im Bank to test the data included in FMS-NG.
3. Identify and assess Ex-Im Bank's contingency plan if FMS-NG is a "no-go" on the production date.
4. Determine whether Ex-Im Bank complied with its own information technology (IT) testing and implementation policies and procedures, as well as with applicable laws, rules, and regulations.

Scope and Methodology

Cotton & Company performed the audit to determine whether Ex-Im Bank's planning and implementation of FMS-NG was adequate and effective. Specifically, we structured our test procedures to meet the above-listed objectives and to identify how Ex-Im Bank designed its data interfaces and data-conversion processes to mitigate risks in FMS-NG.

We conducted interviews with personnel from the Offices of the Chief Financial Officer (CFO) and the Chief Information Officer (CIO), as well as with personnel from Creoal Consulting, a consulting firm that Ex-Im Bank contracted to develop and implement FMS-NG. We also reviewed policies, procedures, and practices; reviewed system documentation and evidence; and tested Ex-Im Bank's controls. We fully documented our testing methodology through creation of a planning memorandum and audit work programs.

We conducted the audit on-site at Ex-Im Bank in Washington, DC, as well as remotely at the Cotton & Company office in Alexandria, VA, with fieldwork from September 2014 to January 2015. During our audit, Bank management expressed concerns that the timing of this audit conflicted with other ongoing audits and the implementation of the system, and therefore, restricted its ability to fully assist with this engagement.

Cotton & Company conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS), as established in the Government Accountability Office (GAO)'s *Government Auditing Standards*, December 2011 Revision. Those standards require that we plan and perform the audit to obtain sufficient,

appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We discussed our observations and conclusions with management officials on January 26, 2015, and included their comments where appropriate.

See Appendix A for details regarding applicable federal laws, regulations, policies, and guidance.

Background

Ex-Im Bank is an independent, self-sustaining executive agency and a wholly-owned United States government corporation. Ex-Im Bank's charter, *The Export Import Bank Act of 1945*, as amended through Public Law 112-122, May 30, 2012, states:

> *It is the policy of the United States to foster expansion of exports of manufactured goods, agricultural products, and other goods and services, thereby contributing to the promotion and maintenance of high levels of employment and real income, a commitment to reinvestment and job creation, and the increased development of the productive resources of the United States.*

To fulfill its charter, Ex-Im Bank assumes the credit and country risks that the private sector is unable or unwilling to accept. The Bank provides working capital guarantees, export credit insurance, loan guarantees, and direct loans to counter the export financing provided by foreign governments on behalf of foreign companies and help U.S. exporters remain competitive.

The Offices of the CFO and the CIO required a more effective financial management system, and in fiscal year (FY) 2012, Ex-Im Bank began a project to replace its legacy financial and administrative IT systems (i.e., the Administrative Accounting Activities (AAA) and Loans Guarantee (LGA) systems). The Bank determined that it required a commercial-off-the-shelf (COTS) solution that had been tailored to the federal government, was certified by the Financial Systems Integration Office (FSIO), and was compliant with credit reform. The Bank ultimately selected Oracle Federal Financials and Oracle Loans as the solution. This project is known as FMS-NG.

The FMS-NG development and production environment is cloud-based and is hosted at Oracle's Managed Cloud Services (MCS) facility in Austin, Texas. The project followed a 23-month implementation schedule and was deployed in October 2014. Ex-Im Bank divided the project into six phases:

- Phase 0 – Finance and Administration
- Phase 1 – Analysis of Alternatives
- Phase 2 – Requirements and Configuration
- Phase 3 – Custom Module Development
- Phase 4 – User Acceptance Testing (UAT)

- Phase 5 – Transition and Go-Live

Ex-Im Bank planned to implement the following application modules:

- Oracle Federal Financials General Ledger (GL)
- Oracle Federal Financials Accounts Payable (AP)
- Oracle Federal Financials Accounts Receivable (AR)
- Oracle Federal Financials Budget Execution (BE)
- Oracle Federal Financials Purchasing (PO)
- Oracle Loans (LNS)

The project also included a 3-month post-production support period to assist with the transition to FMS-NG. In accordance with the established project plan, FMS-NG became live and operational in October 2014.

RESULTS

During our audit, we did not identify any significant issues or major risks that would prevent the implementation of FMS-NG. We noted that the Bank committed senior level personnel to significant components of the implementation effort. Furthermore, we noted that the Bank had adequate processes for documenting and tracking changes to the system and ensuring appropriate security for system interfaces. However, we found that improvements could be made with the planning and documentation of the implementation of FMS-NG. Specifically, Ex-Im Bank did not develop and maintain comprehensive project plans and supporting documentation to ensure that the migration to FMS-NG fully adhered to established plans and that business operations could continue without significant complications. While the Bank developed high-level project plans, the plans did not always include the associated procedures for carrying out the plans. Furthermore, the Bank did not continuously update its plans to ensure they were accurate and reflected required changes. Overall, it was very difficult for the audit team to identify and follow the planned and performed procedures. Documentation was not organized and readily available, and we found that the procedures that were performed did not always tie back to the planning documents. Specifically, the Bank:

- Did not sufficiently plan and document the data-conversion process.
- Did not perform adequate security assessment and authorization (SA&A) activities for FMS-NG access controls, including:
    - developing and documenting account management procedures for granting access to the application both during the initial implementation and once the application was live, and
    - adequately identifying and documenting separation-of-duties requirements for roles within the application.
- Did not develop a contingency plan in the event the system was a "no-go" on the production date or had issues, constraints, or errors during the implementation that prevented it from operating effectively.

The above weaknesses represent increased risks to the Bank's overall ability to promptly identify the root cause of errors and defects in the data; process routine transactions; understand security vulnerabilities and internal control weaknesses in the system; and identify and address issues, constraints or errors in the system. As a result, Ex-Im Bank's normal operations could be delayed or impaired. For example, we identified that purchase card payments and travel reimbursements were not paid in a timely manner and Ex-Im Bank financial reports were delayed. These areas require increased attention as system implementation continues and during future audits.

We made seven recommendations to address the above issues. These recommendations, if implemented, should reduce the risks associated with Ex-Im Bank's implementation of FMS-NG. Ex-Im Bank management agreed with our recommendations and presented actions to address them. Ex-Im Bank management's responses to the findings identified in our audit are included within the report and in Appendix B. We did not audit Ex-Im Bank management's responses, and accordingly, we express no opinion on them.

Finding: Ex-Im Bank Did Not Sufficiently Plan and Document the Data Conversion Process

Ex-Im Bank did not sufficiently plan and document its data conversion activities for the implementation of FMS-NG. The documentation provided for data conversion, testing and cleansing was not always comprehensive or complete. Moreover, the documentation was not organized and readily available which made it difficult to perform the audit and understand the data conversion processes for FMS-NG implementation.

Ex-Im Bank prepared high-level data conversion plans, some data validation test plans, and committed senior personnel to key conversion planning and validation efforts. While we were able to gain an understanding of the data conversion planning and validation efforts through the high-level planning documentation, interviews, walkthroughs, and the validation results provided by the Bank, we found:

- While Ex-Im Bank maintained high-level validation methodologies for validating converted loans, guarantees, claims, and obligations data, similar documentation was not prepared for other validations and reconciliations performed, to include GL conversion and loans fees. In addition, the validation methodologies that the Bank did document only included the general validation approach. For example, Ex-Im Bank noted that it planned to select statistical samples of converted loans, guarantees, claims, and obligations and verify that the sampled items matched legacy data. It also planned to select statistical samples from the legacy data and determine if sample items were properly converted. These methodologies, however, did not describe what attributes would be tested or provide detailed test procedures. Instead, verbal instructions were given to experienced CFO personnel who were the Subject Matter Experts (SME) that performed converted loans, guarantees, claims, and obligations validations. Although the Bank provided details of the completed validations performed by the SMEs, the lack of detailed validation plans and clear procedures increases the risk that testing may not have been properly performed.

- While Ex-Im Bank provided more than 25 data conversion validations that had been completed at the time the Bank responded to our request, we were not provided the conversion test plan or a list of planned or completed validations. As a result, we were unable to determine whether the validations provided were sufficient to validate the data in the new system. Ex-Im Bank did not centrally or consistently monitor and track data-conversion errors, validation results, and the status of

corrective actions. The process used to track data-conversion errors and open issues varied depending on the type of data, the type of validation performed, and the subject matter experts that validated the data. Some errors were communicated and discussed through email, weekly status meetings, or other ad hoc meetings; other errors were documented in individual data validation sheets; and others were tracked on internal activity logs. For example, during the GL conversion process, Ex-Im Bank tracked and approved changes to crosswalks, mappings, and error corrections using email communication between the FMS-NG team and CFO personnel. These emails were not saved in a central location. Without a consistent monitoring and tracking process, unauthorized changes or errors may occur and may not be detected timely.

- Ex-Im Bank did not sufficiently document its data cleansing procedures, prior to converting data to FMS-NG. While data cleansing activities were limited because the Bank only converted open loans, guarantees, claims, and obligations; GL balances for the two prior fiscal years; and customers and vendors that had open agreements or that were active during the prior fiscal year, not properly documenting data cleansing procedures increases the risk that erroneous or unnecessary legacy data could be migrated to FMS-NG and not detected timely.

The above weaknesses exist because Ex-Im Bank did not adequately plan and document the FMS-NG implementation data-conversion activities. Without clear and complete plans and documentation, there is an increased risk that data may not be properly converted and errors or defects may not be detected and corrected timely. This could impair Ex-Im Bank's ability to process routine transactions and cause the Bank's normal operations to be delayed.

The following guidance is relevant to this control activity:

GAO's *Standards for Internal Control in the Federal Government* (2014) states:

> *Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives, such as the process of adhering to requirements for budget development and execution. They help ensure that actions are taken to address risks. Control activities are an integral part of an entity's planning, implementing, reviewing, and accountability for stewardship of government resources and achieving effective results.*
>
> *Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, reconciliations, performance reviews, maintenance of security, and the creation and maintenance of related records which provide evidence of execution of these activities as well as appropriate documentation. Control activities may be applied in a computerized information system environment or through manual processes.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

We recommend that the Chief Financial Officer and Chief Information Officer:

1. Ensure that Ex-Im Bank appropriately plans and documents data-conversion activities for future system implementations, including at a minimum, preparing data conversion and test plans with detailed procedures for how the data will be converted, tested, and cleansed.

2. Gather and save key evidence of FMS-NG data-conversion activities, such as detailed tie-outs of converted data, data maps and crosswalks used, approvals, and logs of errors and their resolution.

3. For the FMS-NG project and future system implementations, centrally organize and maintain all planning, converting, testing and implementation documentation so that it is readily available when needed and for third party review.

Management's Response:

Management concurs with all three recommendations. The Bank will document procedures for data-conversion activities for future system implementations in its "Best Practices" guidance. Specifically, the "Best Practices" will include guidance on planning data-conversion activities; filing and retention of those data-conversion activities; and the organization and maintenance of the planning, converting, testing, and implementation documentation for FMS-NG and future implementations. Lastly, the "Best Practices" will include lessons learned from the Bank's experience with the implementation of FMS-NG. The "Best Practices" guidance will be completed no later than June 30, 2016.

Evaluation of Management's Response:

Management's proposed actions are responsive to the recommendations. Therefore, the recommendations are considered resolved and will be closed upon completion and verification of the proposed actions.

Finding: Ex-Im Bank Did Not Perform Adequate Security Assessment and Authorization Procedures over FMS-NG Access Controls

Controls are not adequate to ensure that Ex-Im Bank performed appropriate Security Assessment and Authorization (SA&A) procedures over FMS-NG access controls. Specifically, we reviewed the system security plan (SSP) that Ex-Im Bank developed to address its National Institute of Standards and Technology (NIST) control responsibilities and its subsequent control testing to validate control implementation. We found that the

SSP was very high-level and did not discuss the details of the in-place controls. As a result, we noted that the following access control issues were not addressed within the SSP or the control testing matrices:

- Ex-Im Bank has not documented its account management procedures for granting access to FMS-NG. While we found that the Bank does have a process to grant users access to FMS-NG, it is an informal process whereby the Controller and the Treasurer are the only individuals permitted to authorize access to the system. The authorizations are performed through email. This process has not been documented and is not consistent with the Bank's procedures for granting new users access to other systems, which requires the completion of an access request form to determine what level of access is being requested.

- Ex-Im Bank has not identified, documented, and implemented separation-of-duties requirements for FMS-NG system administrators. As a result, we identified one user that appeared to have excessive access within the application as this individual was assigned both system administrator and financial operation functions.

Without performing an appropriate SA&A over access controls for new systems, management may not have a clear understanding of the risks present in their environment such as security vulnerabilities and internal control weakness throughout the financial management system

The following guidance is relevant to this control activity:

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization, dated April 2013,* states:

> ***PL-2 System Security Plan***
>
> *The organization:*
>
> *a. Develops a security plan for the information system that:*
>
> 1. *Is consistent with the organization's enterprise architecture;*
> 2. *Explicitly defines the authorization boundary for the system;*
> 3. *Describes the operational context of the information system in terms of missions and business processes;*
> 4. *Provides the security categorization of the information system including supporting rationale;*
> 5. *Describes the operational environment for the information system and relationships with or connections to other information systems;*
> 6. *Provides an overview of the security requirements for the system;*
> 7. *Identifies any relevant overlays, if applicable;*

8. *Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and*
9. *Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;*

CA-2 Security Assessments

The organization:

a. Develops a security assessment plan that describes the scope of the assessment including:

- Security controls and control enhancements under assessment;

- Assessment procedures to be used to determine security control effectiveness; and

- Assessment environment, assessment team, and assessment roles and responsibilities;

b. Assesses the security controls in the information system [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;

c. Produces a security assessment report that documents the results of the assessment; and

d. Provides the results of the security control assessment, in writing, to the authorizing official or authorizing official designated representative.

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

We recommend that the CFO and CIO:

4. Document formal account management procedures for the request, approval, creation, review, and removal of FMS-NG accounts.

5. Develop and implement an access request form to facilitate the account management process for FMS-NG.

6. Develop and implement separation-of-duties requirements for FMS-NG administrators.

Management's Response:

Management concurs with all three recommendations. The Bank has formally documented the account management procedures for accessing FMS-NG in the "FMS-NG Operations Manual" dated January 2015 and updated the Bank's "Building and Systems Access Request Form" to include FMS-NG. The Bank provided a description of the administrator's responsibilities for access control for FMS-NG. It is the Bank's position that the user profiles are typical to this Oracle product and that the access to financial information reflects government and commercial practices. The Bank requested a re-evaluation of the FMS-NG administrators' responsibilities by an expert with the technical expertise and understanding of this Oracle system.

Evaluation of Management's Response:

Management's proposed actions are responsive to the recommendations. The OIG will re-evaluate the separation-of-duties requirement for FMS-NG administrators before concluding on this recommendation. The remaining recommendations are considered resolved and will be closed upon completion and verification of the proposed actions.

Finding: Ex-Im Bank Did Not Document a Contingency Plan to Address Risks Associated with Post-Implementation Issues

Ex-Im Bank did not develop, document, or test a contingency plan to address risks related to implementing a new financial system. While management stated that they had determined courses of action for handling issues that might arise both before and after the implementation of FMS-NG, we were unable to obtain any evidence demonstrating that those actions were appropriately considered and validated. For example, there was no evidence Ex-Im Bank considered the resource constraints that would result from the implementation of FMS-NG. During our audit, we found that the Bank did not identify and address that additional staffing would be needed to perform the necessary manual data entry and to process transactions when the system was first implemented.

As a result of not having a contingency plan, several issues arose as part of the system roll-out that were not timely addressed. These issues included:

- Purchase card payments were not paid in a timely manner. As a result, an Ex-Im Bank purchase card was suspended.
- Travel reimbursements were not paid in a timely manner. As a result, several Bank employees remained unpaid for up to four months.
- Ex-Im Bank financial reports were delayed.

We found that the purchase card suspension and late travel voucher payments resulted from a backlog of unprocessed transactions that accrued during the system conversion. The

Bank lacked sufficient staff resources to manually process these financial transactions in a timely manner. Since management did not develop a contingency plan, it did not identify and address potential issues, constraints or errors that could occur, such as those described above.

The following guidance is relevant to this control activity:

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organization, dated April 2013,* states:

> ***CP-2 Contingency Plan***
> *The organization:*
> *a. Develops a contingency plan for the information system that:*
> 1. *Identifies essential missions and business functions and associated contingency requirements;*
> 2. *Provides recovery objectives, restoration priorities, and metrics;*
> 3. *Addresses contingency roles, responsibilities, assigned individuals with contact information;*
> 4. *Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;*
> 5. *Addresses eventual, full information system restoration without deterioration of the security safeguards originally planned and implemented; and*
> 6. *Is reviewed and approved by [Assignment: organization-defined personnel or roles];*
>
> *b. Distributes copies of the contingency plan to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements];*
> *c. Coordinates contingency planning activities with incident handling activities;*
> *d. Reviews the contingency plan for the information system [Assignment: organization-defined frequency];*
> *e. Updates the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing;*
> *f. Communicates contingency plan changes to [Assignment: organization-defined key contingency personnel (identified by name and/or by role) and organizational elements]; and*
> *g. Protects the contingency plan from unauthorized disclosure and modification.*

Recommendation, Management's Response, and Evaluation of Management's Response

Recommendation:

We recommend that the CFO and CIO:

7. For current and future system implementations, develop and document contingencies for essential functions in the event that they do not operate effectively post-implementation.

Management's Response:

Management concurs with this recommendation. The Bank will create a document folder of lessons learned from the Bank's experience with the 2014 FMS-NG implementation. This effort will be completed no later than June 30, 2016.

Evaluation of Management's Response:

Management's proposed action is responsive to the recommendation. Therefore, the recommendation is considered resolved and will be closed upon completion and verification of the proposed actions.

APPENDIX A

Federal Laws, Regulations, Policies, and Guidance

As part of our tests of controls, we reviewed Ex-Im Bank's compliance with applicable federal laws and regulations related to information system controls, including but not limited to:

- **GAO's *Standards for Internal Control in the Federal Government* (1999)**
- **GAO's *Internal Control Management and Evaluation Tool* (August 2001) (GAO-01-1008G)**
- NIST SPs and Federal Information Processing Standards (FIPS), particularly:
    - SP 800-53, Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*
    - SP 800-53A, Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*
    - SP 800-34, Rev. 1, *Contingency Planning Guide for Federal Information Systems*
    - SP 800-37, Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*
    - SP 800-30, *Risk Management Guide for Information Technology Systems*
    - SP 800-65, *Integrating IT Security into the Capital Planning and Investment Control Process*
    - FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*

Management Comments

EXPORT-IMPORT BANK
OF THE UNITED STATES

March 24, 2015

Michael McCarthy
Deputy Inspector General
Office of the Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Washington, DC 20571

Dear Mr. McCarthy,

Thank you for providing the Export-Import Bank of the United States ("Ex-Im Bank" or "the Bank") Management with the Office of the Inspector General's ("OIG") "Independent Auditor's Report on the Export-Import Bank's Planning and Implementation of the Financial Management System – Next Generation (FMS-NG)", dated March 4, 2015 (the "report"). Management continues to support the OIG's work, which complements the Bank's efforts to continually improve its processes. Ex-Im Bank is proud of the strong and cooperative relationship it has with the OIG.

The OIG contracted with Cotton & Company, LLP ("Cotton") to conduct a performance audit of the Bank's planning and implementation process of FMS-NG. The Bank appreciates Cotton acknowledging that during its review they did not "identify any significant issues or major risks that would prevent the implementation of FMS-NG." The Bank is also pleased that the report acknowledges that the Bank "had adequate processes for documenting and tracking changes to the system and ensuring appropriate security for system interfaces."

The OIG, through Cotton, has made seven recommendations they believe will improve upon the Bank's systems planning and implementation procedures. The Bank concurs with the seven recommendations, and has already taken action to address two of the recommendations. At the time of the audit, the Bank had also already taken the recommended actions regarding a third recommendation. We will move forward with implementing the four remaining recommendations this fiscal year.

1

811 VERMONT AVENUE, N.W. WASHINGTON, D.C. 20571

The report mentions that the Bank did not fully participate with the audit, stating the Bank "restricted its ability to fully assist with this engagement." As explained to representatives from Cotton at the entrance conference which occurred on September 2, 2014, their audit was beginning at a time when two major events were occurring that required significant staff resources. The first was the end of the fiscal year, which is arguably the busiest time of the year for our Chief Financial Officer's team and it entails enormous amounts of detailed staff work to ensure the books are accurately closed out for the year. The second was that in parallel to the end of the fiscal year responsibilities, we were rolling out the new financial management system. When they layered on top of this their audit, it presented significant staff availability challenges. In short, the Bank was already faced with priorities including closing its fiscal year-end books, the on-going OIG financial statement audit, testing and implementing the new FMS-NG system, and performing day-to-day functions in accordance with the Bank's mission. Even with those challenges, the Bank was still committed to assisting the auditors to the greatest extent possible and the report acknowledges that "the Bank committed senior level personnel to significant components of the implementation effort."

Recommendation 1: Ensure that Ex-Im Bank appropriately plans and documents data-conversion activities for future system implementations, including at a minimum, preparing data conversion and test plans with detailed procedures for how the data will be converted, tested, and cleansed.

Management Response: The Bank concurs with this recommendation.

During the 23-month development and implementation of FMS-NG, the Bank's specialized Oracle systems contractor, Creoal Consulting ("Creoal"), established various processes and procedures for the Bank, including data conversion plans, which were designed to ensure that the scope and methods of FMS-NG met the project objectives. In addition to these high-level plans, the Bank followed established contingencies, procedures and methodologies for testing and implementing FMS-NG.

In October 2014, FMS-NG was fully implemented and became operational in accordance with the Bank's established plans. Following the implementation, Creoal provided hands-on support to the Bank for a period of three months. As previously mentioned in this response and in the report, Cotton "did not identify any significant issues or major risks that would prevent the implementation of FMS-NG" and noted that "the Bank committed senior level personnel to significant components of the implementation effort" and that "the Bank had adequate processes for documenting and tracking changes to the system and ensuring appropriate security for system interfaces."

The Bank will document procedures for data-conversion activities for future system implementations. These "Best Practices" will include guidance on planning data-conversion

activities, as well as lessons learned from the Bank's experience with the implementation of FMS-NG. The Bank expects this to be completed in the first half of FY 2016.

Recommendation 2: Gather and save key evidence of FMS-NG data-conversion activities, such as detailed tie-outs of converted data, data maps and crosswalks used, approvals, and logs of errors and their resolution.

Management Response: The Bank concurs with the recommendation.

As stated in the Bank's response to Recommendation 1 above, the Bank followed established contingencies, procedures and methodologies for testing and implementing FMS-NG. The Bank, working with Creoal, provided a great deal of evidence to Cotton regarding conversion activities undertaken throughout the planning and implementation process. The Bank will continue to gather and save additional evidence of its data-conversion activities. The "Best Practices" will provide guidance on the filing and retention of those data-conversion activities.

Recommendation 3: For the FMS-NG project and future system implementations, centrally organize and maintain all planning, converting, testing and implementation documentation so that it is readily available when needed and for third party review.

Management Response: The Bank concurs with this recommendation.

The Bank's "Best Practices" will provide guidance on the organization and maintenance of the FMS-NG planning, converting, testing, and implementation documentation, as well as for future implementations. The Bank expects this to be completed in the first half of 2016.

Recommendation 4: Document formal account management procedures for the request, approval, creation, review, and removal of FMS-NG accounts.

Management Response: The Bank concurs with this recommendation.

The Bank currently has in place account management procedures for accessing FMS-NG. The Bank has formally documented the procedures in the "*FMS-NG Operations Manual,*" dated January 2015, which provides guidance on how FMS-NG accounts are requested, created, reviewed and removed.

Recommendation 5: Develop and implement an access request form to facilitate the account management process for FMS-NG.

Management Response: The Bank concurs with this recommendation.

The Bank has developed and implemented a formal process for requesting FMS-NG accounts. At the time the audit report was issued, the Bank was in the process of updating the access request form, "*Building and Systems Access Request Form*" to include FMS-NG. The form was updated February 12, 2015 and placed on EXIMConnect.

Recommendation 6: Develop and implement separation-of-duties requirements for FMS-NG administrators.

Management Response: The Bank concurs with this recommendation, and at the time of the audit, the Bank had developed and implemented separation-of-duties requirements for FMS-NG administrators to make sure users do not overlap functions and responsibilities. Below is a description of the administrators' responsibilities for access control with respect to FMS-NG:

A System Administrator is responsible for controlling access to Oracle Applications and assuring smooth ongoing operation. For each site where Oracle Applications is installed, the system administrator shall follow the following tasks:

- Manage and control security - decide which users have access to each application, and within an application, which forms, functions, and reports a user can access;
- Set up new users - register new Oracle Applications users and give them access to only those forms, functions and reports they need to do their jobs. Areas of responsibility include:
    a. FMS-NG CRM Resource Manager – responsible for creating a CRM Resource for each person who will access the CRM modules (e.g. Loans);
    b. FMS-NG HRMS Manager – responsible for creating an Oracle person that is associated with the FMS-NG User; and
    c. FMS-NG Purchasing Manager – responsible for creating and granting access to Purchasing Buyers (FMS-NG users with Oracle Purchasing Buyer functions).
- Audit user activity - monitor what users are doing and when they do it and choosing who to audit and what type of data to audit;
- Set user profiles - set user profile values at the site, application, responsibility, and user levels; and
- Manage concurrent processing - monitor and control concurrent processing using a few simple forms.

The Bank has worked closely with Creoal to ensure that the user profiles are typical of this Oracle product and that the access to financial information that crosses business lines or functions that a user profile may represent also reflect government and commercial practice for this product. Creoal is implementing this product in accordance with Oracle's default

mechanisms as the product comes off-the-shelf. The Bank requests that this recommendation and the actions taken by the Bank are re-evaluated by an expert with the technical expertise and understanding of this Oracle system.

Recommendation 7: For current and future system implementations, develop and document contingencies for essential functions in the event that they do not operate effectively post-implementation.

Management Response: The Bank concurs with this recommendation.

The Bank will create a document folder of lessons learned from the Bank's experience with the 2014 FMS-NG implementation. The Bank expects this to be completed in the first half of FY 2016.

As recognized in the relevant finding of the report, the Bank had a "Big Picture" contingency plan in place. In the event FMS-NG failed to operate as planned, the Bank's fall back option was to postpone the live implementation of FMS-NG and continue to use the Bank's legacy Financial Management System until issues were resolved. The Bank also had detailed "manual" procedures in case system interfaces failed to work.

We thank the OIG for your efforts to ensure the Bank's policies and procedures continue to improve, as well as the work you do with us to protect Ex-Im funds from fraud, waste, and abuse. We look forward to strengthening our working relationship and continuing to work closely with the Office of the Inspector General.

Sincerely,

Charles J. Hall
Executive Vice President and Chief Risk Officer
Export-Import Bank of the United States

To Report Fraud, Waste, or Abuse, Please Contact:

Email: IGhotline@exim.gov

Telephone: 1-888-OIG-Ex-Im (1-888-644-3946)

Fax: (202) 565-3988

Address: Office of Inspector General
Export-Import Bank of the United States
811 Vermont Avenue, NW
Suite 138
Washington, DC 20571

Comments and Suggestions

If you wish to comment on the quality or usefulness of this report or suggest ideas for future audits please contact Terry Settle, Acting Assistant Inspector General for Audits, at Terry.Settle@exim.gov or call (202) 565-3498. Comments, suggestions, and requests can also be mailed to the attention of the Assistant Inspector General for Audits at the address listed above.

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