



July 2018

EXPORT-IMPORT BANK

The Bank Needs to Continue to Improve Fraud Risk Management

Accessible Version

GAO Highlights

Highlights of [GAO-18-492](#), a report to congressional committees

Why GAO Did This Study

According to the Bank, it serves as a financier of last resort for U.S. firms seeking to sell to foreign buyers but that cannot obtain private financing for their deals. Its programs support tens of thousands of American jobs and enable billions of dollars in U.S. export sales annually, the Bank says. The Bank is also backed by the full faith and credit of the United States government, meaning that taxpayers could be responsible for Bank losses.

The Export-Import Bank Reform Reauthorization Act of 2015 included a provision for GAO to review the Bank's antifraud controls within 4 years, and every 4 years thereafter. This report examines the extent to which the Bank has adopted the four components of GAO's Fraud Risk Framework—commit to combating fraud; regularly assess fraud risks; design a corresponding antifraud strategy with relevant controls; and evaluate outcomes and adapt. GAO reviewed Bank documentation; interviewed a range of Bank managers; and surveyed Bank employees about the extent to which the Bank has established an organizational culture and structure conducive to fraud risk management.

What GAO Recommends

GAO makes seven recommendations, centering on conducting a fraud risk assessment, tailored to the Bank's operations, to serve as the basis for the design and evaluation of appropriate antifraud controls. The Bank agreed with GAO's recommendations, saying it will take steps to improve its fraud risk management activities.

View [GAO-18-492](#). For more information, contact Seto J. Bagdoyan at (202) 512-6722 or bagdoyans@gao.gov.

July 2018

EXPORT-IMPORT BANK

The Bank Needs to Continue to Improve Fraud Risk Management

What GAO Found

In managing its vulnerability to fraud, the Export-Import Bank of the United States (the Bank) has adopted some aspects of GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework). This framework describes leading practices in four components: organizational culture, assessment of inherent program risks, design of tailored antifraud controls, and evaluation of outcomes. As provided in the framework, for example, the Bank has identified a dedicated entity within the Bank to lead fraud risk management. GAO also found that Bank managers and staff generally hold positive views of the Bank's antifraud culture. However, GAO also found that management and staff hold differing views on key aspects of that culture. These differing views include how active the Bank should be in addressing fraud. For example, Bank managers told GAO the Bank's current approach has been appropriate for dealing with fraud. However, about one-third of Bank staff responding to a GAO employee survey said the Bank should be "much more active" or "somewhat more active" in preventing, detecting, and addressing fraud. These and other divergent views indicate an opportunity to better ensure the Bank sets an antifraud tone that permeates the organizational culture, as provided in the Fraud Risk Framework.

GAO found the Bank has taken some steps to assess fraud risk. For example, the Bank's practice has generally been to assess particular fraud risks and lessons learned following specific instances of fraud encountered, according to Bank managers. However, the Bank has not conducted a comprehensive fraud risk assessment, as provided in the framework. The Bank has also been compiling a "register" of risks identified across the organization, including fraud. This register, however, does not include some known methods of fraud, such as submission of fraudulent documentation, thus indicating it is incomplete. Without planning and conducting regular fraud risk assessments as called for in the framework, the Bank is vulnerable to failing to identify fraud risks that can damage its reputation or harm its ability to support U.S. jobs through greater exports. As provided in the framework, managers should determine where fraud can occur and the types of internal and external fraud the program faces, including an assessment of the likelihood and impact of fraud risks inherent to the program.

At the conclusion of GAO's review, Bank managers said they will fully adopt the GAO framework. They said they plan to complete a fraud risk assessment by December 2018, and to determine the Bank's fraud risk profile—that is, document key findings and conclusions from the assessment—by February 2019. Work to adopt other framework components will begin afterward, the managers said. However, they did not provide details of how their efforts will be in accord with leading practices of the framework. As a result, GAO makes framework-specific recommendations in order to enumerate relevant issues and to present clear benchmarks for assessing Bank progress. This complete listing of recommendations is important in light of the Bank's recent embrace of the framework; recent changes in Bank leadership; and expected congressional consideration of the Bank's reauthorization in 2019.

Contents

| | | |
|--|--|----|
| Letter | | 1 |
| | Background | 3 |
| | The Bank Has Identified a Dedicated Entity to Lead Fraud Risk Management, but Management and Staff Disagree on Aspects of an Antifraud Culture | 13 |
| | The Bank Has Taken Some Steps to Assess Known Fraud Risks but Has Not Conducted a Comprehensive Fraud Risk Assessment | 22 |
| | The Bank Has Instituted Some Antifraud Controls but Not Developed a Strategy Based on a Fraud Risk Assessment, and Has Opportunities to Improve Fraud Awareness and Data Analytics | 35 |
| | The Bank Has Opportunities to Improve Monitoring and Evaluating Outcomes of Its Fraud Risk Management Activities | 47 |
| | Conclusions | 48 |
| | Recommendations for Executive Action | 51 |
| | Agency Comments and Our Evaluation | 52 |
| <hr/> | | |
| Appendix I: Objectives, Scope, and Methodology | | 57 |
| Appendix II: Results of GAO Survey of Bank Employees: “Anti-Fraud Controls at the Export-Import Bank of the United States” | | 61 |
| Appendix III: Comments from the Export-Import Bank of the United States | | 75 |
| Appendix IV: GAO Contact and Staff Acknowledgments | | 85 |
| Appendix V: Accessible Data | | 86 |
| | Data Table | 86 |
| | Agency Comment Letter | 86 |
| <hr/> | | |
| Table | Table 1: Claims Paid for Medium- and Short-Term Products, Export-Import Bank of the United States, Fiscal Years 2008–2017 | 31 |

Figures

| | |
|--|----|
| Figure 1: Major Types of Financing Provided by the Export-Import Bank of the United States | 6 |
| Figure 2: Export-Import Bank of the United States Exposure by Product Type, Geographic Region, and Economic Sector, Fiscal Year 2017 | 7 |
| Figure 3: The GAO Fraud Risk Management Framework | 11 |
| Figure 4: Export-Import Bank of the United States, Operational Risks—Likelihood vs. Impact | 29 |
| Figure 5: Selected Export-Import Bank of the United States Evaluations Prior to Transaction Approval | 38 |
| Figure 6: Export-Import Bank of the United States Monitoring of Transactions after Approval | 39 |
| Accessible Data for Figure 2: Export-Import Bank of the United States Exposure by Product Type, Geographic Region, and Economic Sector, Fiscal Year 2017 | 86 |

Abbreviations

| | |
|----------------------|---|
| CRC | Credit Review and Compliance division |
| CRO | chief risk officer |
| Fraud Risk Framework | <i>A Framework for Managing Fraud Risks in Federal Programs</i> |
| Green Book | <i>Standards for Internal Control in the Federal Government</i> |
| OGC | Office of the General Counsel |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| SVP | senior vice president |
| the Bank | Export-Import Bank of the United States |
| the Board | Board of Directors |

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.



July 19, 2018

Congressional Committees

The mission of the Export-Import Bank of the United States (the Bank) is to support American jobs by facilitating the export of U.S. goods and services. According to the Bank, it serves as a financier of last resort for U.S. companies that are seeking to sell to foreign buyers but that cannot obtain private financing for their deals—thus assuming credit and country risks the private sector is unable or unwilling to accept.¹ To support these exports, the Bank offers loan, loan guarantee, and insurance programs. According to the Bank, its programs support tens of thousands of American jobs and enable billions of dollars in U.S. export sales annually.

The Bank is backed by the full faith and credit of the United States government, meaning that taxpayers could be responsible for losses arising from Bank operations.² Since 2011, the Bank’s congressionally authorized exposure limit—the total amount it may have outstanding in credit and insurance authority—has increased from \$100 billion and now stands at \$135 billion. Total actual exposure as of September 30, 2017, was \$72.5 billion. By number, a large majority of Bank transactions involve smaller companies and smaller amounts of assistance.³ By dollar amount, however, large transactions dominate activity, according to the Bank.

The Bank requires periodic reauthorization from Congress. Congress last did so in 2015,⁴ after debate that included discussion of fraud risks at the

¹The Bank is a corporation that serves as the export credit agency of the United States. See, 12 U.S.C. § 635. It is a wholly owned government corporation, as defined in 31 U.S.C. § 9101(3)(C).

²The Bank told us it sets aside reserves to cover all expected losses, so that it would only be in extreme circumstances that taxpayers would be responsible for Bank losses.

³See a discussion of various Bank issues, including the nature of Bank transactions, at Congressional Research Service, *Export-Import Bank: Frequently Asked Questions*, R43671 (Washington, D.C.: Apr. 13, 2016).

⁴Export-Import Bank Reform Reauthorization Act of 2015, Pub. L. No. 114-94, div. E, title LI, 129 Stat. 1312, 1763-71 (2015). The Bank’s current authorization expires on September 30, 2019. The Bank’s authority to approve transactions lapsed from July 1, 2015, through December 4, 2015, a period when Congress had not reauthorized the Bank.

Bank.⁵ As part of its 2015 reauthorization, Congress included a provision in the statute for us to review the adequacy of design and effectiveness of the Bank's antifraud controls, within 4 years of reauthorization, and every 4 years thereafter.⁶

This report examines the Bank's management of fraud risks in its export credit activities, by evaluating the extent to which the Bank has adopted the four components described in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).⁷ Specifically, we evaluate the extent to which the Bank has (1) established an organizational culture and structure conducive to fraud risk management; (2) planned regular fraud risk assessments and assessed risks to determine a fraud risk profile; (3) designed and implemented a strategy with specific control activities to mitigate assessed fraud risks; and (4) evaluated outcomes using a risk-based approach and adapted activities to improve fraud risk management.⁸

To evaluate the extent to which the Bank has adopted the components described in GAO's Fraud Risk Framework, we assessed Bank fraud risk management practices against provisions of the framework, which also incorporates concepts from *Standards for Internal Control in the Federal Government* (also known as the "Green Book").⁹ We reviewed Bank policy and governance documentation, plus other documentation; reviewed GAO and Bank Office of the Inspector General (OIG) reports on fraud and fraud risk management topics; and interviewed a range of Bank

⁵Discussion of fraud risk included a Bank employee's guilty plea in federal court to charges of bribery, among other misconduct. According to the Bank's Office of the Inspector General (OIG), the former loan officer pleaded guilty to one count of bribery of a public official, for accepting more than \$78,000 in bribes in return for recommending the approval of unqualified loan applications to the Bank.

⁶See 12 U.S.C. § 635a-6(b).

⁷GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015). Each of the Fraud Risk Framework's four *components* is broken down into *overarching concepts*, which in turn include *leading practices* that demonstrate ways for program managers to carry out the overarching concepts. We use the components / overarching concepts / leading practices nomenclature throughout this report.

⁸We are also preparing a second report that will include an examination of a sample of Bank transactions, as provided in the 2015 reauthorization.

⁹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

managers, at both the senior-management level and those overseeing relevant Bank operating units.¹⁰ We also surveyed Bank employees about their perceptions of the Bank’s organizational culture and attitudes toward fraud and fraud risk management. Specifically, we surveyed all non-senior-management Bank employees (that is, those below the level of senior vice president, who are responsible for implementing, but not determining, Bank policy), and obtained a sufficient response rate—73.5 percent—to capture a range of employee views. We present tallies of survey results for particular questions, as well as individual comments, in the main text of this report based on their relevance to the respective subject matter. See appendix I for a full discussion of our scope and methodology, including our survey methodology. Complete results of our survey are presented in appendix II.

We conducted this performance audit from October 2016 to July 2018 in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Background

Export credit agencies such as the Bank are usually government agencies, although some private institutions operate export credit programs on their respective governments’ behalf, according to a Bank report on global export credit competition. These agencies offer financing for domestic companies to make sales to foreign buyers, in the form of products such as loans, guarantees, and insurance for exporters, according to the Organisation for Economic Co-operation and Development, which monitors international export credit activity.

¹⁰In this report, we refer collectively to these Bank personnel as “Bank managers.” We interviewed Bank employees as relevant to our objectives from across the Bank, including at the senior vice president level; chief personnel by function, such as chief financial officer; and others responsible for individual business units.

The Bank is one of several federal agencies promoting U.S. exports.¹¹ According to the Bank, as of December 31, 2016, it had identified 96 export credit agencies worldwide. There have been significant changes in the role of export credit agencies since 2007 and the global financial crisis and the European debt crisis, according to the Bank. This is because ready access to credit before the global financial crisis has given way to caution in lending among private-sector banks, and also because other nations have adopted export credit agencies as a tool for national growth.

For fiscal year 2014—which the Bank says is the most recent year in which it operated with full authority¹²— the Bank reported authorizing nearly \$20.5 billion in financing in support of an estimated \$27.5 billion worth of U.S. exports and nearly 165,000 American jobs. For fiscal year 2017, operating under reduced authority, the Bank reported authorizing more than \$3.4 billion in financing to support \$7.4 billion of exports and an estimated 40,000 jobs.

The Bank, which has about 430 employees, was established under the Export-Import Bank Act of 1945.¹³ Under the act, the Bank must have a “reasonable assurance” of repayment when providing financing; it must supplement, and not compete with, private capital; and it must provide terms that are competitive with foreign export credit agencies. Also relevant to whether the Bank provides assistance is whether foreign competitors of the U.S. exporter are receiving export credit assistance from their home nations, and thus the American exporter would need assistance to stay competitive. Over time, Congress has directed the Bank to support certain specific types of exports. Such requirements include using at least 25 percent of its authority to finance small-business

¹¹In addition to the Bank, the U.S. Department of Agriculture provides financing for American agricultural exports. The Small Business Administration provides guarantees for small-business exports. The Overseas Private Investment Corporation provides financing for U.S. exports in developing economies in support of U.S. foreign policy objectives.

¹²As noted earlier, the Bank’s authority to approve transactions lapsed from July 1, 2015, through December 4, 2015, when Congress did not reauthorize the Bank. In addition, as described later, the Bank’s Board of Directors (the Board) lost a quorum, and with that, the ability to approve certain transactions.

¹³Pub. L. No. 79-173, 59 Stat. 526 (1945), codified as amended at 12 U.S.C. § 635 et seq.





exports; promoting exports related to renewable energy sources; and promoting financing for sub-Saharan Africa.¹⁴

Bank Product Types

As described in figure 1, to support U.S. exports, the Bank offers four major types of financing: direct loans, loan guarantees, export-credit insurance, and working capital guarantees. Bank products generally have three maturity periods: Short-term transactions are for less than 1 year; medium-term transactions are from 1 to 7 years long; and long-term transactions are more than 7 years.

¹⁴The Export-Import Bank Act of 1945 has been amended over the years to add various requirements. They include a requirement for the Bank to make available at least 25 percent of its total authority to finance exports by small businesses for fiscal year 2016 and each following year (added by the Export-Import Bank Reform and Reauthorization Act of 2015, Pub. L. No. 114-94 (2015)); renewable energy requirements (added by the Export-Import Bank Reauthorization Act of 2002, Pub. L. No. 107-189 (2002)); and a sub-Saharan Africa requirement (added by the Export-Import Bank Reauthorization Act of 1997, Pub. L. No. 105-121 (1997)).

Figure 1: Major Types of Financing Provided by the Export-Import Bank of the United States

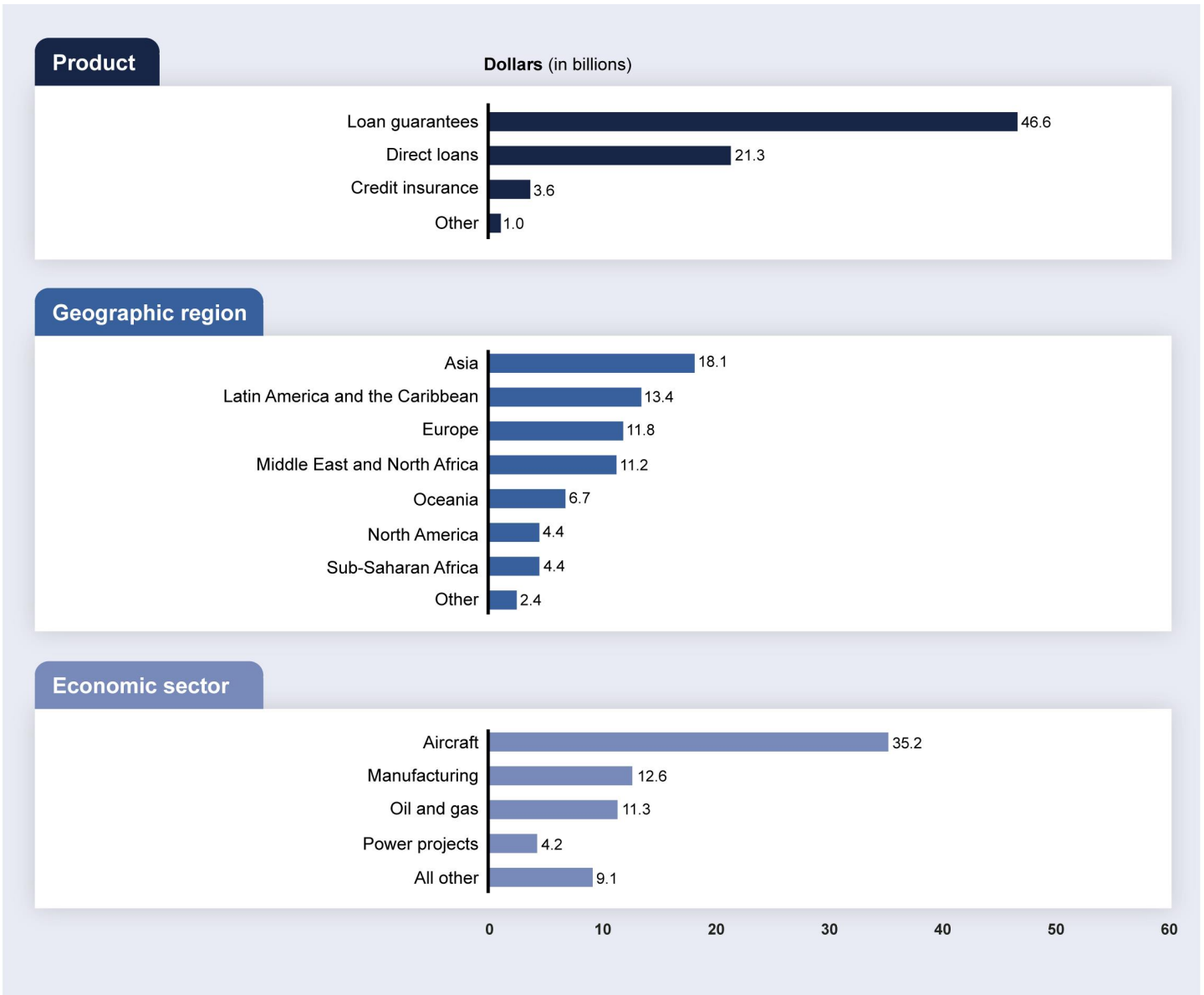
| Type of financing | Description |
|---|--|
|  Direct loan | The Export-Import Bank of the United States (the Bank) lends money to a foreign buyer, to finance the buyer’s purchase of goods or services from a U.S. exporter. |
|  Loan guarantee | A private-sector financial institution lends money to a foreign buyer of U.S. goods or services, and the Bank guarantees repayment of the loan to the financial institution. |
|  Credit insurance | The Bank insures payments due to a U.S. exporter or lender after sale of goods or services to a foreign buyer. |
|  Working capital | A form of loan guarantee. The Bank guarantees loans by private lenders to U.S. exporters for working capital funds, which are used to produce or market goods and services for export. |

Source: Export-Import Bank of the United States, Congressional Research Service. | GAO-18-492

For fiscal year 2017, the Bank reported it had exposure in 166 countries.¹⁵ Figure 2 shows Bank exposure by product type, geographic region, and economic sector, for fiscal year 2017. Its greatest exposure, by product type, was in loan guarantees. By geographic region, the largest exposure was the Asian market. By economic sector, exposure was biggest in aircraft products.

¹⁵For financial statement and analytical purposes, the Bank defines exposure as the authorized outstanding and undisbursed principal balance of loans, guarantees, and insurance, also including any unrecovered balances of payments made on claims submitted and approved by the Bank. Export-Import Bank of the United States, *2017 Annual Report* (Washington, D.C.).

Figure 2: Export-Import Bank of the United States Exposure by Product Type, Geographic Region, and Economic Sector, Fiscal Year 2017



Source: Export-Import Bank of the United States. | GAO-18-492

Because the Bank’s mission is to support U.S. jobs through exports, there are foreign-content eligibility criteria and limitations on the level of foreign

content that may be included in a Bank financing package.¹⁶ For medium- and long-term transactions, for example, the Bank limits its support to 85 percent of the value of goods and services in a U.S. supply contract, or 100 percent of the U.S. content of an export contract, whichever is less. There are also requirements that certain products supported by the Bank must be shipped only on U.S.-flagged vessels.

Defaults occur when transaction participants fail to meet their financial obligations. The Bank must report default rates to Congress quarterly.¹⁷ It calculates the default rate as overdue payments divided by financing provided.¹⁸ If the rate is 2 percent or more for a quarter, the Bank may not exceed the amount of loans, guarantees, and insurance outstanding on the last day of that quarter until the rate falls under 2 percent. As of March 31, 2018, the Bank reported its default rate at 0.438 percent.¹⁹

Bank Board of Directors and Vacancies

The Bank is overseen by a Board of Directors (the Board), which has a key role in approving Bank transactions, because directors must approve medium- and long-term transactions of greater than \$10 million.²⁰ Since July 2015, however, the Board has lacked a quorum (at least three

¹⁶“Content” is the amount of domestic and foreign cost of labor, materials, overhead, and other inputs associated with the production of an export.

¹⁷12 U.S.C. § 635g.

¹⁸Specifically, the default rate is “total amount of required payments that are overdue (claims paid on guarantees and insurance transactions, plus loans past due)” divided by “total amount of financing involved (disbursements).”

¹⁹The rate is calculated as: overdue payments of \$546.1 million divided by total financing of \$124.8 billion. See Export-Import Bank of the United States, *Default Rate Report As of March 2018*. In addition, some default rates by geography or line of business vary considerably from the overall rate. For example, for Oceania (Australia, New Zealand, and Papua New Guinea), the rate was 1.68 percent as of March 2018, and in the Bank’s mandated “environmentally beneficial” line of business, the rate was 4.17 percent.

²⁰The Board has five members—the Bank’s president serves as chairman of the Board, its first vice president serves as vice chairman, and three additional members are appointed; all have 4-year terms. Board members are nominated by the President and subject to Senate confirmation. 12 U.S.C. §635a(c). Once appointed, directors serve at the pleasure of the President.

members), which has precluded approval of these large transactions.²¹ Also due to the lack of a quorum, new transaction activity has shifted away from larger transactions, according to Bank managers.

The Bank's total exposure has recently declined by about a third, from \$113.8 billion at the end of fiscal year 2013 to \$72.5 billion at the close of fiscal year 2017, according to the Bank. In part during the period when the Board has lacked a quorum and been unable to approve large transactions, the amount of earnings the Bank has transferred to the Department of the Treasury has declined steadily, according to Bank figures. Since 2012, the amount the Bank transferred to the Treasury peaked at \$1.1 billion in fiscal year 2013. In successive years, that transfer fell to \$674.7 million in fiscal year 2014, \$431.6 million in fiscal year 2015, and \$283.9 million in fiscal year 2016, before reaching zero in fiscal year 2017. As the Board vacancies have continued, a backlog of Board-level transactions has grown, reaching an estimated \$42.2 billion as of December 2017.²²

The Board also has a key role in risk management, with members serving on the Bank's Risk Management Committee, which oversees portfolio stress testing and risk exposure, according to the Bank. Board members also approve the appointment of the chief risk officer (CRO), the chief ethics officer, and members of advisory committees.

During the course of our review, in addition to the Board quorum issue, Bank senior leadership changed. According to the Bank, the following took place: The acting chairman of the Board and president of the Bank resigned. The vice chairman, first vice president, and acting agency head also later resigned. Subsequently, a new executive vice president, chief operating officer, and acting agency head was named. Following that, an acting president and Board chairman was named.

²¹Smaller transactions can be approved by Bank staff, under authority delegated by the Board. Although the bulk of all Bank transactions have been below the \$10 million threshold, transactions requiring Board approval have accounted for about two-thirds of all Bank financing, by dollar volume, according to the Bank.

²²About 84 percent of the backlog, or \$35.4 billion, is in the Bank's power and oil and gas/commodities categories, according to the Bank. The backlog is entirely in long-term transactions, and there has been no backlog in medium- and short-term transactions, according to Bank managers.

Fraud Risk Management Standards and Guidance

Fraud and “fraud risk” are distinct concepts. *Fraud*—obtaining something of value through willful misrepresentation—is challenging to detect because of its deceptive nature. *Fraud risk* exists when individuals have an opportunity to engage in fraudulent activity, have an incentive or are under pressure to commit fraud, or are able to rationalize committing fraud. When fraud risks can be identified and mitigated, fraud may be less likely to occur. Although the occurrence of fraud indicates there is a fraud risk, a fraud risk can exist even if actual fraud has not yet been identified or occurred.²³

According to federal standards and guidance, executive-branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. Federal internal control standards call for agency management officials to assess the internal and external risks their entities face as they seek to achieve their objectives. The standards state that as part of this overall assessment, management should consider the potential for fraud when identifying, analyzing, and responding to risks.²⁴ Risk management is a formal and disciplined practice for addressing risk and reducing it to an acceptable level.²⁵

We issued our Fraud Risk Framework in July 2015. The Fraud Risk Framework provides a comprehensive set of leading practices, arranged in four components, which serve as a guide for agency managers developing efforts to combat fraud in a strategic, risk-based manner. The Fraud Risk Framework is also aligned with Principle 8 (“Assess Fraud Risk”) of the Green Book.²⁶ The Fraud Risk Framework describes leading practices in four components: *commit*, *assess*, *design and implement*, and *evaluate and adapt*, as depicted in figure 3.

²³For further details on the nature of fraud and fraud risk, see, for example, GAO, *Medicare and Medicaid: CMS Needs to Fully Align Its Antifraud Efforts with the Fraud Risk Framework*, [GAO-18-88](#) (Washington, D.C.: Dec. 5, 2017).

²⁴[GAO-14-704G](#).

²⁵MITRE, *Government-wide Payment Integrity: New Approaches and Solutions Needed* (McLean, Va.: February 2016).

²⁶The Bank is not subject to 31 U.S.C. § 3512, which requires executive agencies to follow the Green Book, because it is a government-owned corporation. Bank managers told us the Bank voluntarily seeks to follow Green Book Principle 8.

Figure 3: The GAO Fraud Risk Management Framework



Source: GAO. | GAO-18-492

The Fraud Reduction and Data Analytics Act of 2015, enacted in June 2016, requires the Office of Management and Budget (OMB) to establish guidelines for federal agencies to create controls to identify and assess fraud risks, and to design and implement antifraud control activities. The act also requires OMB to incorporate the leading practices of the Fraud Risk Framework in those guidelines. In July 2016, OMB published guidance on enterprise risk management and internal controls in federal executive departments and agencies.²⁷ Among other things, this guidance affirms that managers should adhere to the leading practices identified in the Fraud Risk Framework. The act also requires federal agencies to submit to Congress a progress report each year, for 3 consecutive years, on implementation of the controls established under the OMB guidelines.

²⁷See Office of Management and Budget Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016).

The Bank Has Identified a Dedicated Entity to Lead Fraud Risk Management, but Management and Staff Disagree on Aspects of an Antifraud Culture

The Bank has identified a dedicated entity to lead fraud risk management activities, as called for in the first component of GAO’s Fraud Risk Framework. In addition, employees generally have a positive view of antifraud efforts across the Bank, according to our employee survey.²⁸ However, we also found that management and staff have differing views on key aspects of the Bank’s antifraud culture. In particular, we identified issues inconsistent with the notion of “an antifraud tone that permeates the organizational culture,” as the Fraud Risk Framework calls for,²⁹ in which there is agreement across the organization on key fraud issues and practices. These areas of disagreement on aspects of the Bank’s antifraud culture include how active the Bank should be in preventing, detecting, and addressing fraud; and the adequacy of time for underwriting, which the Bank says is its primary safeguard against fraud. Bank managers said that our findings provide an opportunity for additional staff training on fraud issues.

Fraud Risk Framework Component 1:

Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management



Source: GAO. | GAO-18-492

²⁸For a description of survey methodology, see app. I.

²⁹Our evaluation criteria in this section—dedicated entity and antifraud culture—are the two overarching concepts of the first component of GAO’s Fraud Risk Framework.

The Bank Has Identified a Dedicated Entity to Lead Fraud Risk Management Activities

The Bank has identified two managers who serve as a dedicated entity for leading fraud risk management activities, managers told us. These are a vice president of the Credit Review and Compliance division (CRC) and an assistant general counsel in the Bank's Office of the General Counsel (OGC). According to Bank managers, they work together under the direction of the CRO, who was permanently named to the position on a part-time basis in September 2016.³⁰ GAO's Fraud Risk Framework provides that the dedicated entity can be an individual or a team, depending on the needs of the agency. Hence, the Bank's arrangement is consistent with the framework. Before recently identifying the two managers as the dedicated entity, Bank managers told us there was no centralized entity responsible for fraud risk management. Likewise, Bank written procedures, dated February 2015, for preventing, detecting, and prosecuting fraud provided there is no "central figure in charge" of such efforts. The CRO told us that he oversees the two managers in their work as the dedicated entity.

We also found that the two managers named to form the dedicated entity are involved in one of the key activities contemplated by the Fraud Risk Framework. Overall, these activities include serving as a repository of knowledge on fraud risks and controls; leading or assisting with trainings and other fraud-awareness activities; and coordinating antifraud initiatives.³¹ The two managers have helped develop and provide training, some of which is mandatory and targeted directly at fraud issues, managers told us. The Bank provides semiannual fraud training through OGC for claims-processing staff, Bank managers also said. Other training, while nominally not directed at fraud, can nevertheless involve

³⁰Under the terms of its 2015 reauthorization, Congress required the Bank to create the current CRO position. 12 U.S.C. §635a(l). In January 2016, the Bank appointed an acting CRO, who was permanently named to the position in September 2016, on a part-time basis. The CRO is also senior vice president of credit and risk management, according to the Bank, and in that role is responsible for overseeing credit policy, credit review and compliance, country risk and economic analysis, and engineering and environmental analysis. The Bank noted that before the current CRO was named, the position was also filled from November 2013 to December 2015.

³¹We selected these leading practices for review here based on relevancy, following discussions with Bank managers, review of Bank documents, and results obtained from our employee survey; as well as to describe Bank antifraud efforts.

fraud issues, Bank managers told us. For instance, managers told us recent training on shipping matters included a review of fraudulent shipping documentation, which is one way fraud can be perpetrated.³²

Bank Managers and Staff Express Positive Views of Antifraud Culture, but They Hold Different Views on Key Aspects of That Culture

GAO's Fraud Risk Framework calls for creating an organizational culture to combat fraud, such as by demonstrating senior-level commitment to fighting fraud and involving all levels of the agency in setting an antifraud tone.³³ Bank managers, in interviews, and staff, in our employee survey, generally expressed positive views of the Bank's antifraud culture.³⁴ For example, according to Bank managers, the Bank has maintained an antifraud culture, which they attribute to factors including: fraud and ethics training; internal controls; tone set at the top by management; a realization after fraud cases in the 2000s that the Bank cannot be solely reactive to fraud; and the pursuit of fraud cases by the Bank and its OIG.

Our survey results indicate that Bank employees also generally have a positive view of antifraud tone across the Bank and attention paid to combating fraud. For example:

³²In addition to this training, Bank managers told us OGC has also offered semiannual fraud training for the Asset Management Division, and fraud training at the Bank's annual conference. According to managers, in 2014 and 2015, the Bank offered a 1-day fraud-awareness training provided by an external vendor. Further, the OIG conducts fraud presentations at internal Bank staff meetings, they also said.

³³Senior-level commitment and involving all levels of the agency are leading practices under the Fraud Risk Framework's antifraud culture overarching component. We selected these leading practices for review based on relevancy, following discussions with Bank managers and compiling results of our employee survey.

³⁴Because culture ultimately reflects beliefs and perceptions of those in the organization, and not necessarily the representations of senior managers, we conducted our survey of Bank employees below the level of senior management.

- Eighty percent said Bank management in general has established a clear antifraud tone, to the extent of “a great deal” or “a lot.”³⁵
- Employees said that based on senior management’s actions, preventing, detecting, and addressing fraud is “extremely” or “very” important to the Bank (86 percent).
- Staff expressed “a great deal” or “a lot” of confidence in senior management (76 percent), managers in their division (85 percent), and their peers (82 percent), to respond to fraud on a timely and appropriate basis.

Illustrative Comments from GAO’s Survey of Bank Employees

- “The Bank has become much more sensitized to the risks of fraud over the last 10 years.”
- “The progress made on combating fraud is tremendous. When I started, no one really cared, and fraud was common.... Now, blatant attempts at fraud are a rarity.”
- “There is a high degree of concern at all levels of the Bank regarding potential fraud, which has resulted in good oversight.”

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Note: For selected questions, GAO’s employee survey provided an opportunity for written comments. Respondent comments shown here, and those following throughout this report, are taken from those narrative responses, in order to illustrate aggregate survey findings.

We also found indications of disagreement among managers and staff about how active the Bank should be in preventing, detecting, and addressing fraud. Overall, Bank managers told us, the Bank’s current approach has been appropriate for dealing with fraud. In particular, an OGC manager told us that with its underwriting and due diligence standards—the process for assessing and evaluating an application before approval—and established fraud procedures, the Bank has an appropriate strategy to mitigate fraud risks it knows about or envisions occurring. However, about one-third of survey respondents (35 percent) said the Bank should be “much more active” or “somewhat more active” in preventing, detecting, and addressing fraud. Less than half (44 percent) said the current level of activity should remain the same.³⁶ Asked whether

³⁵For a complete tally of employee survey results, as well as question wording and response options, see app. II. In general, the survey questions allowed respondents to select an answer from among several points along a high-to-low range. For this question, for example, employees could select from this range of responses: “a great deal,” “a lot,” “some,” “a little,” “not at all,” or “unsure/don’t know.” The appendix lists the number of valid responses for each question. As described in detail in app. I, there were 403 employees in our survey population, and we received 296 responses.

³⁶Remaining responses were “somewhat less active” (2 percent) and “unsure/don’t know” (19 percent).

what they see as the Bank’s current approach for overseeing fraud and fraud risk, based on the level of responsibilities of various parties involved, is the most effective way to do so, about 6 in 10 (62 percent) said yes.³⁷ While Bank managers characterized our survey results as positive, these divergent views indicate room for strengthening antifraud culture, in light of the Fraud Risk Framework’s goal of achieving shared views across the organization.

Illustrative Comments from GAO’s Survey of Bank Employees

- “The Bank should be much more active in preventing, detecting, and addressing fraud, because the Bank handles business transactions that involve taxpayers’ money.”
- “The Bank needs more funding for technology to help with fraud prevention and additional Bank staff to spot/monitor fraud.”
- “The first- and second-level managers have not done all they could to ensure fraud prevention. The front-line credit officers are the ones in the best position to detect fraud and management does not always support it.”
- “A more proactive approach to fraud detection, rather than a reactive approach, would be more prudent. This means trying to sniff out fraud [at] the preapplication and underwriting stages.”

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Another area where we identified differing views is in the adequacy of time for underwriting. Preapproval underwriting, and the due diligence done as part of that process, is the Bank’s main control against fraud, according to Bank managers and procedures.³⁸ However, during our review, Bank managers also acknowledged in interviews that their business involves potentially competing objectives: performing sufficient due diligence to prevent and detect fraud prior to approving transactions,

³⁷Remaining responses were “no” (7 percent) and “unsure/don’t know” (31 percent). The parties about which we queried were: OGC, the OIG, Office of Risk Management, Bank senior management, all bank staff and managers, and other.

³⁸As noted, in this report, we refer collectively to the following as “Bank managers”: Bank employees as relevant to our objectives from across the Bank, including at the senior vice president level; chief personnel by function, such as chief risk officer; and program, unit, or division managers.

while still processing transactions in a timely manner to meet customers' needs and achieve the Bank's mission.³⁹

Some comments we received in our employee survey illustrated the tension between the competing objectives of thorough due diligence and timely processing of transactions.

Illustrative Comments from GAO's Survey of Bank Employees

- "Detecting fraud is a very high priority, as is appropriate. But overemphasis on managing that risk would lead to a sense of paranoia when approaching any new risk."
- "Given all the other obligations we have, even more time spent on fraud detection means less time for other transaction-related work, with only marginal benefit."
- "Risk is part of the business, and being overly cautious leads to never taking any risk and consequently not serving the customers."
- "Fraud is important to discuss, but it should not become the main force driving the organization. There needs to be more of a risk-based analysis when determining how much to concentrate on fraud."

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

According to a Bank report on global export credit competition, transaction processing time is an important factor in customers' decisions to choose the Bank over foreign export-financing agencies.⁴⁰ In recent years, the Bank has significantly reduced processing time. Bank statistics show that the percentage of transactions completed in 30 days or fewer grew from 57 percent in fiscal year 2009 to 91 percent in fiscal year 2016. For 100 days or fewer, the rate has increased from 90 percent to 99 percent over the same period.

Bank managers told us they seek to strike the right balance between the competing objectives and believe they have done so. For example, according to the CRC division, the Bank chooses to perform some of its fraud-detection and mitigation activities after application approval—such as through reviews of transactions selected on both a random and risk-based basis—in order to not unduly delay processing applications. Under

³⁹The Fraud Risk Framework acknowledges that managers may see a conflict between fulfilling program mission and safeguarding public resources. However, the framework also indicates that the purpose of proactively managing fraud risk is to facilitate, not hinder, program mission and goals, by helping to ensure that government services achieve their intended purposes.

⁴⁰Export-Import Bank of the United States, *Export-Import Bank of the United States, Report to the U.S. Congress on Global Export Credit Competition* (June 2017).

Bank practices, document review can be abbreviated,⁴¹ and, after underwriting approval, lenders may accept certain transaction documentation, such as invoices or shipping documents, at face value unless something appears suspicious, managers told us. In the particular case of processing short- and medium-term transactions, the Bank is alert to “red flag” items—known warning signs, such as use of nonbank financial institutions, or participants that are trading entities rather than original equipment manufacturers, managers told us. But otherwise, the Bank limits the extent of its application investigation, according to the Bank’s OGC. In particular, as the Bank’s OGC told us, the Bank is required by law to make medium-term offerings a “simple product.”⁴² There is pressure both legally and commercially to process transactions quickly, because, otherwise, an exporter could lose its business opportunity, the Bank’s OGC told us. In many of these transactions, both the exporter and buyer are small, the OGC also said, so it is more difficult to get information. As a result, according to the OGC, the Bank relies more on self-reporting by transaction parties. For these reasons, the Bank’s OGC told us, for both short- and medium-term products, there are not as many “inherent checks and balances” in the process. We note that based on previous GAO work, self-reporting can present an opportunity for fraud.

However, our survey results suggest that significant portions of Bank staff question whether the Bank is striking the right balance in providing sufficient time for preapproval review of transactions. Specifically, Bank staff raised concerns about the amount of time dedicated to the key task of preapproval review of applications. For each of the Bank’s three major product maturity categories, we asked whether the application process provides enough time for Bank staff to conduct thorough due diligence on potential fraud risks. For short-term products—which Bank managers said, as a category in general, have been the most susceptible to fraud recently—less than half (47 percent) said there is “always” or “usually” enough time; and about 20 percent said there is “sometimes,” “seldom,”

⁴¹Bank antifraud procedures direct that loan officers and underwriters are not to check authenticity of all documents “so as to provide the efficiency necessary to allow exporters to compete with their foreign competitors.”

⁴²See, 12 U.S.C. § 635(a).

or “never” enough time.⁴³ For both medium- and long-term products, about 6 in 10 (56 percent and 61 percent, respectively) said the application process “always” or “usually” provides enough time.⁴⁴ As noted, while Bank managers characterized our survey results as positive, these views indicate an opportunity for the Bank to further set an antifraud tone that permeates the organizational culture.⁴⁵

Illustrative Comments from GAO’s Survey of Bank Employees

- “More due diligence should be required in order to qualify for the U.S. government’s support.”
- “The Bank is more concerned with increasing sales than preventing fraud.”

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Our survey also identified that while nearly half (48 percent) of respondents rated fraud as a “very significant” or “significant” risk to the Bank, there may be misunderstanding among employees on where responsibility lies for fraud risk management. We asked employees to describe the extent to which each of six offices or groups—OGC, the OIG, the Office of Risk Management, Bank senior management, all bank staff and managers collectively, or others—are responsible for overseeing fraud risk management activities at the Bank. The OIG received the highest response, with 73 percent saying it has “a great deal of responsibility.” Bank managers told us this result is to be expected, because staff associate issues of fraud with the OIG. However, these survey results suggest confusion—lack of a shared view, from the standpoint of antifraud culture—around the OIG’s role, which includes investigating suspected fraud, rather than overseeing the Bank’s fraud

⁴³The remaining responses were “unsure/don’t know” (33 percent). Respondents could indicate whether this question is applicable to their job or experience. Results reported here exclude those who said the question is not applicable. The number of respondents on that basis was 174.

⁴⁴For medium-term products, 11 percent said there is “sometimes,” “seldom,” or “never” enough time; 33 percent of respondents said they were unsure or did not know. For long-term products, 5 percent said there is “sometimes,” “seldom,” or “never” enough time; 34 percent said they were unsure or did not know. Respondents could indicate whether this question is applicable to their job or experience. Results reported here exclude those who said the question is not applicable. The numbers of respondents on that basis were 168 and 178, respectively.

⁴⁵An examination of any particular control, such as preapproval review of applications, was outside the scope of our work. We discuss the preapproval review issue here to illustrate varying perceptions as a matter of organizational culture.

risk management activities.⁴⁶ The OIG acknowledged to us that its role does not include responsibility for overseeing fraud risk management activities at the Bank.⁴⁷

Asked about our findings overall, Bank managers told us they view our survey results as positive because the results indicate employees have a strong awareness of fraud and the risk it presents to the Bank. For example, regarding the results about the role of the OIG, they noted that staff are actively encouraged to report suspected fraud through channels—first to OGC, for subsequent referral to the OIG. Thus, employees would understand the OIG as being responsive to fraud, and Bank managers believe this likely accounts for the survey result.

Nevertheless, they said, our survey results provide an opportunity for more detailed training, to better communicate with staff. In particular, the Bank managers told us such training would focus on the Bank’s approach to fraud, plus the Bank’s organizational structure for addressing fraud. The training will also clarify that the OIG has an investigative function as well as an auditing function, they said. Our employee survey results underscore the potential benefit of further fraud training. Among respondents who said they have received fraud or fraud risk-related training provided by the Bank in the last 2 years, three-quarters said it was “extremely” or “very” relevant to their job duties. Nearly two-thirds (63 percent) said it was “extremely” or “very” useful to their duties. Overall, about half (52 percent) of respondents said fraud or fraud risk-related information obtained from management, or any Bank resources, has increased their understanding of fraud “a great deal” or “a lot.”

The differences we identified in perceptions of fraud risk and fraud management responsibilities do not, by themselves, implicate the performance of any particular antifraud control, or suggest that any additional control is necessary. However, to the extent views on

⁴⁶An examination of particular division of responsibilities for overseeing fraud risk management was outside the scope of our work. We discuss this issue here to illustrate varying perceptions as a matter of organizational culture and the extent of shared understanding across the organization on key antifraud matters.

⁴⁷Specifically, according to the OIG, its mission 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.”

significant antifraud issues, such as how active the Bank should be in preventing, detecting, and addressing fraud, or adequacy of time devoted to underwriting, differ across the organization, the Bank cannot ensure that it is best setting an antifraud tone that permeates the organizational culture, as provided in the Fraud Risk Framework. In particular, as the framework describes, antifraud tone and culture are important parts of effective fraud risk management. These elements can provide an imperative among peers within an organization to address fraud risks, rather than have the organization rely solely on top-down directives.

The Bank Has Taken Some Steps to Assess Known Fraud Risks but Has Not Conducted a Comprehensive Fraud Risk Assessment

The Bank has taken some steps to assess fraud risk. However, it has not conducted a fraud risk assessment, tailored to its operations, or created a fraud risk profile, both as provided in the second component of GAO's Fraud Risk Framework.⁴⁸ Further, under the framework, recent changes in the Bank's operating environment indicate a heightened need to do so.

⁴⁸The evaluation criteria here—tailored fraud risk assessment and creation of a fraud risk profile—are the two overarching concepts of the second component of GAO's Fraud Risk Framework. The fraud risk profile represents the key findings and conclusions of the fraud risk assessment, and is an essential part of overall antifraud strategy. There is no universally accepted approach for conducting fraud risk assessments, since circumstances between programs vary. However, assessing fraud risks generally involves five actions:

- identifying inherent fraud risks affecting the program—that is, determining where fraud can occur and the types of both internal and external fraud risks the program faces;
- assessing the likelihood and impact of inherent fraud risks;
- determining fraud risk tolerance;
- examining the suitability of existing fraud controls and prioritizing risk that remains after application of the existing fraud controls; and
- documenting the program's risk profile.

For details, see [GAO-15-593SP](#), p. 12. The Fraud Risk Framework does not recommend a standard interval between fraud risk assessments. In general, allowing extended periods to pass between fraud risk assessments could result in ineffective control activities. According to experts GAO consulted, the frequency of updates can range from 1 to 5 years.

We also found that although the Bank has been compiling a “risk register” intended to catalog risks it faces across the organization, this compilation does not include some known fraud risks, indicating that the Bank’s assessment is incomplete. In addition, we found that while the Bank has adopted a general position on the degree of risk it will tolerate, its current risk tolerance is not specific and measurable, as provided by federal internal control standards. Bank managers told us they will revise their fraud risk management practices to fully adopt the Fraud Risk Framework.

The Bank Has Taken Some Steps to Assess Known Fraud Risks but Does Not Conduct Regular, Comprehensive Fraud Risk Assessments

A leading practice of the Fraud Risk Framework calls for agencies to conduct fraud risk assessments at regular intervals, as well as when there are changes to the program or operating environment, because assessing fraud risks is an iterative process.⁴⁹ Managers should determine where fraud can occur and the types of internal and external fraud the program faces. This includes an assessment of the likelihood and impact of fraud risks inherent to the program; that is, meaning both fraud risks known through fraud that has been experienced, as well as other fraud risk that can be identified, based on the nature of the program.

Fraud Risk Framework Component 2:

Plan regular fraud risk assessments and assess risks to determine a fraud risk profile

⁴⁹We selected this leading practice for review based on relevancy, following discussions with Bank managers, and as logically related to the overarching concept of conducting regular fraud assessments that are tailored to the program.



Source: GAO. | GAO-18-492

According to a Bank report, *FY2016 Enterprise Risk Assessment*, the Bank is more susceptible to fraud, due to “the nature of the Bank’s mission, the high volume of transactions it executes, and the need for various groups within the Bank to work together to successfully defend against fraud.”⁵⁰ The Bank’s short- and medium-term products are more susceptible to fraud, according to Bank managers. Other indicators of fraud, according to the managers, include domestic geography,⁵¹ transactions that involve truck shipments; international geography, since conducting adequate due diligence can be more difficult in remote locations; and when there are smaller, less well-known parties on both sides of the transaction.⁵²

In this environment, the Bank has taken some steps to assess known fraud risks. Generally, the Bank’s practice has been to assess particular fraud risks and lessons learned following specific instances of fraud encountered, according to Bank managers. Because it has focused on fraud already encountered, the Bank’s practice has not been of the comprehensive nature provided in the Fraud Risk Framework.

As an example of its current approach, according to Bank managers, the Bank experienced “significant fraud” in the early 2000s. This was chiefly in the medium-term program, and to a lesser degree, the short-term program, the managers said.⁵³ As a result, the Bank made changes that

⁵⁰Export-Import Bank of the United States, *Export-Import Bank of the United States of America, FY 2016 Enterprise Risk Assessment* (Mar. 17, 2017), p. 6.

⁵¹For example, transactions in the areas of Miami, Florida, or El Paso, Texas, where higher instances of fraud have been observed.

⁵²According to Bank managers, long-term transactions, by contrast, are typically large projects (such as aircraft), in which established, experienced participants are less likely to fall victim to fraud.

⁵³In particular, the Bank suffered from two large fraud cases in the early 2000s, according to managers. The Bank paid \$93 million in claims arising from one case, known as the San Antonio Trade Group matter, and \$80 million in claims arising from the second case, known as the Philippines matter. According to the Bank, these cases resulted from a decision to expand the Bank’s medium- and short-term offerings “down-market”—that is, to offer them to less-creditworthy participants. Bank managers told us the Bank was aware at the time of increased *credit* risk that would come with the move, but in hindsight, did not appreciate increased *fraud* risk that also came with the expansion. It took several years for the Bank to put into place its current system to address fraud risk, they said.

reduced the fraud significantly, they said.⁵⁴ Otherwise, according to the CRO, fraud has been addressed within product lines, as appropriate.⁵⁵ Under its current approach, the Bank's risk assessments do not include areas where fraud has not already been detected, according to Bank managers.⁵⁶ They acknowledged that approach could expose the Bank to fraud risks for activities not yet discovered.

A key difference between the Bank's current approach, as illustrated above, and leading practices as provided in the Fraud Risk Framework, can be seen in how fraud risks are assessed. As described later, the Bank has been compiling risks it faces across the organization, with fraud risk among them. These efforts have focused on soliciting views of Bank staff. By contrast, the framework envisions a more comprehensive approach. Effective fraud risk assessments identify specific tools, methods, and sources for gathering information about fraud risks, according to the framework. Among other things, this can include data on trends from monitoring and detection activities. Under the framework, programs might develop surveys that specifically address fraud risks and related control activities. It may be possible, the framework suggests, to conduct focus groups, or engage relevant stakeholders, both internal and external, in one-on-one interviews or brainstorming about types of fraud risks.

Thus, we found, the Bank's current process for assessing fraud risk has been generally reactive and episodic, rather than regularly planned and comprehensive. Rather than adopt a more proactive approach, the Bank has instead relied on the normal processing and review of transactions—

⁵⁴For example, according to Bank managers: The Bank worked with law-enforcement agencies to understand how the frauds were perpetrated. An early focus was on how to more quickly identify an emerging fraud problem. The Bank also instituted its database checks of transaction participants; began requiring collateral in most medium-term transactions; required dual approvals of applications; and restricted the term of transactions involving used equipment, which were seen as especially prone to fraud.

⁵⁵In addition, the Bank may also learn of fraud through the regular, postapproval reviews of transactions conducted by the CRC division. These reviews are not specifically geared toward fraud issues, but can nonetheless play a key role in fraud detection, according to the Bank managers. See fig. 6 later in this report.

⁵⁶Bank managers told us the Bank reviews, on a monthly basis, claims, defaults, delinquencies, and impaired credits, and that fraud is a subset of claims. We note, however, that such activities focus on already-identified transactions, and that it may be true that not all fraud cases result in claims or otherwise appear in these categories.

which build in experience with previous fraud schemes—as the truest test for identifying fraud issues or concerns, according to Bank managers.

Recent changes in the Bank’s program and operating environment also heighten the need for comprehensively assessing fraud risks, according to the Fraud Risk Framework. Such changes include the Bank’s inability to approve large transactions due to the absence of a quorum. This has meant transaction activity has shifted to smaller transactions, which carry a greater risk of fraud, according to bank managers. Additionally, Congress recently mandated that the Bank increase its focus on small businesses, whose transactions present a different risk profile than those of the Bank’s large customers, according to Bank managers.⁵⁷ Further, the Bank’s transaction backlog could also become an issue in the future. If a Board quorum is restored, there could be pressure to process transactions quickly in order to clear the backlog, which could undermine the quality of the underwriting process, according to documentation from the Office of the CRO.⁵⁸

According to our review, the Bank’s current antifraud controls further the goal of protecting Bank resources and providing “reasonable assurance” of repayment. However, without planning and conducting regular fraud risk assessments, as identified in GAO’s Fraud Risk Framework, the Bank is vulnerable to not identifying material risks that can hurt performance or its ability to fulfill its mission. As Bank managers acknowledged to us, the Bank faces acute reputational risk if new instances of large or otherwise significant fraud emerge.

The Bank Has Been Working to Identify Major Organizational Risks, but Its Identification of Fraud Risks Is Incomplete

The Bank has taken some steps in an effort to identify, manage, and respond to risks, including those related to fraud. It has been developing a “risk register”—a compilation of risks across the organization. It has

⁵⁷See 12 U.S.C. §635(b)(1)(E)(v), as added by the Export-Import Bank Reform Reauthorization Act of 2015. It directs the Bank to make available at least 25 percent of its loan, guarantee, and insurance authority—up from 20 percent—to directly finance exports by small businesses, beginning in fiscal year 2016 and continuing each year following.

⁵⁸While acknowledging the risk, Bank managers told us the underwriting process and credit standards will not change.

also recently completed an “enterprise risk assessment” through an outside consultant. However, these efforts do not reach the full extent of the relevant leading practices of the Fraud Risk Framework. Specifically, the framework call for agencies to identify inherent fraud risks of a program, examine the suitability of existing fraud controls, and then to prioritize “residual” fraud risks—that is, risks remaining after antifraud controls are adopted.⁵⁹

For the risk register, individual business units contribute items, such as indicating types of risk and likelihood, and methods to mitigate the risk.⁶⁰ The register, through the Bank’s Office of Risk Management, notes the risk of fraudulent deals generally, characterizing the likelihood as “somewhat likely,” but having the possibility of “major” financial, operational, legal, and reputational impacts. However, particular methods of fraud known to the Bank through experience—such as applicants submitting fraudulent documentation—are absent thus far. This indicates the register is incomplete, from the standpoint of identifying where fraud can occur and the types of internal and external fraud risks the program faces, as provided in GAO’s Fraud Risk Framework. Other inherent fraud risks, such as those posed by the Bank’s more limited understanding of transactions made when it delegates lending authority to other institutions, are also absent from its risk register.⁶¹ Work continues on developing the risk register, Bank managers told us. However, adoption of the risk register has been delayed, due to a reorganization of Bank management and the vacancies on the Board.⁶² Without a more comprehensive assessment of inherent fraud risks, the Bank cannot be

⁵⁹We selected these leading practices for review based on relevancy, following discussions with Bank managers and review of Bank documents, and, in particular, as a means to evaluate progress thus far on the risk register.

⁶⁰In addition to fraud risk, other types of risk identified in the register include: cyber threats; antiquated technology; the possibility of the Bank no longer being self-sustaining; and the possibility of a qualified audit opinion for Bank financial statements.

⁶¹Delegated lending authority involves transactions that rely on underwriting by outside lenders. In these transactions, the products handled by the outside lenders carry the same Bank guarantees as the Bank’s own offerings, but the Bank forgoes a complete understanding of the fraud risk associated with the external lender products. For example, in such transactions, the Bank does not require the outside lenders to report instances of fraud, according to Bank managers. The Bank does not require lenders to have any specific antifraud policies—instead relying on the outside lenders’ financial regulators—and is unaware of what instances of fraud have occurred previously.

⁶²Although Board vacancies have delayed adoption, Bank managers told us work has continued in developing a second version of the register, and further meetings have been held to continue discussing risk issues.

assured of the extent to which existing controls effectively mitigate inherent risks.

According to the chief risk officer, the Bank's risk register is part of a more wide-ranging "enterprise risk management" strategy,⁶³ which includes documenting a range of risks across the organization, including fraud.⁶⁴ In March 2017, as part of this strategy, the Bank completed the enterprise risk assessment.⁶⁵ Based on assessments by senior Bank managers, it identifies fraud risk—defined as a "significant and high-profile fraud" conducted against the Bank—as one among a range of risks facing the Bank.⁶⁶ Consistent with Bank managers' representations to us, the enterprise risk assessment ranks the likelihood of fraud risk as low against other risks the Bank faces—fourth out of five among "operational" risks, and 24th out of 26 total identified risks. Figure 4 depicts how the Bank evaluates these operational risks, in a schematic pairing likelihood of the event with expected impact if they were to occur. In this context, fraud risk is the least prominent risk among the top operational risks identified.

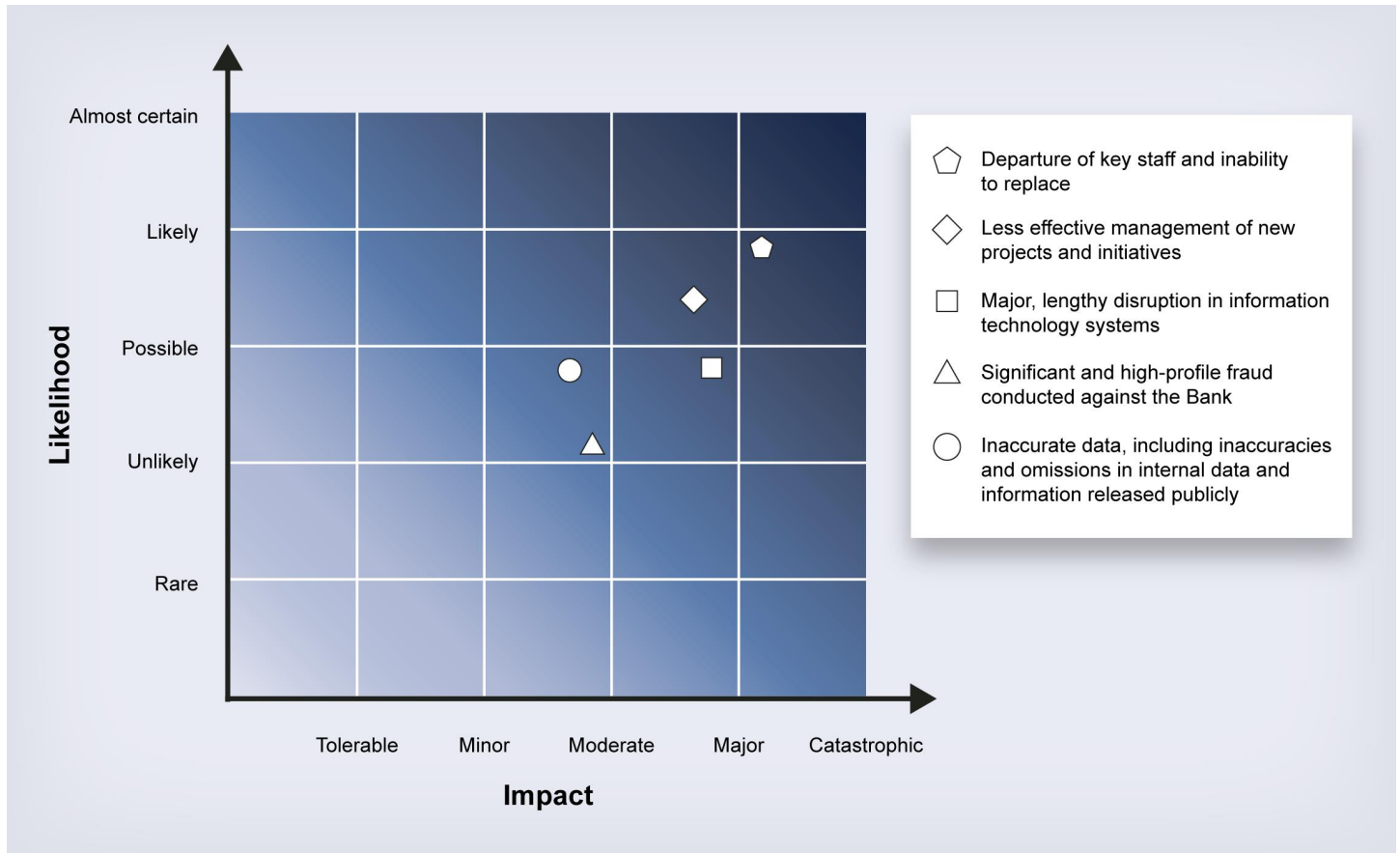
⁶³Enterprise risk management is designed to allow management to understand an organization's portfolio of top-risk exposures, which could affect the organization's success in meeting its goal. As such, enterprise risk management is a decision-making tool that allows leadership to view risks across the organization. Enterprise risk management recognizes how risks interact (for example, how one risk can magnify or offset another risk), and also examines the interaction of actions taken to address a risk, such as acceptance or avoidance. For example, treatment of one risk in one part of the organization can create a new risk elsewhere or can affect the effectiveness of the risk treatment applied to another risk.

⁶⁴For example, according to a "Risk Appetite Statement" adopted in 2015, major risk areas for the Bank include credit risk, strategic risk, market risk, and operational risk, which includes fraud risk. The largest single risk the Bank faces is credit risk, Bank managers told us. Market risk includes factors such as adverse changes in interest rates, availability and cost of debt capital, and asset prices.

⁶⁵*Export-Import Bank of the United States of America, FY 2016 Enterprise Risk Assessment.*

⁶⁶As noted, the assessment is based on senior managers' views. According to the Bank's March 2017 report, those interviewed did not include line staff involved in fraud prevention and detection. As discussed later in this report, we recommend that wider perspectives be considered when assessing fraud risk.

Figure 4: Export-Import Bank of the United States, Operational Risks—Likelihood vs. Impact



Source: GAO adaptation of information from Export-Import Bank of the United States (the Bank). | GAO-18-492

In addition to operational risks, the enterprise risk assessment also details six high risks facing the Bank overall. Among them are new or unfamiliar deal structures, which may present increased repayment risk; and doing business in new and unfamiliar technologies, sectors, and industries where the Bank has limited experience.⁶⁷ Although fraud is not explicitly identified as a risk, we note these new activities could provide an opening for those seeking to commit fraud.

⁶⁷The other four factors identified were: that Congress will not reauthorize the Bank after current authorization expires in 2019; the Board will lack a quorum; the Bank will not be viewed as a reliable source of credit support, for reasons such as uncertainty over reauthorization; and attrition of key personnel and inability to replace them.

During our review, Bank managers maintained that the enterprise risk assessment represents a “comprehensive fraud risk assessment” undertaken by the Bank. They also, however, acknowledged that this assessment does not contain all the elements of a fraud risk assessment as described in GAO’s Fraud Risk Framework. For instance, as noted, the Bank has not conducted a comprehensive assessment of inherent fraud risks, tailored to its operations.

We note that because, as described above, the Bank has not undertaken a fraud risk assessment as envisioned by the Fraud Risk Framework, its ranking of fraud risk compared to other risks may change after it has completed such an assessment. This is because a comprehensive assessment may identify new fraud risks or produce revised assessments of known fraud risks, both of which could affect relative rankings of other risks.

The Bank’s Fraud Risk Tolerances Are Not Specific and Measurable

A leading practice of the Fraud Risk Framework calls for agencies to determine fraud risk tolerance.⁶⁸ Further, federal internal control standards state that managers should consider defining risk tolerances that are specific and measurable.⁶⁹ In addition, under the framework, tolerance cannot be determined until the agency has identified inherent fraud risks and assessed their likelihood or impact.

As part of its overall risk management activities, the Bank has adopted a general position on its fraud risk tolerance.⁷⁰ Specifically, Bank managers told us that, by its nature, the Bank accepts more risk than the commercial sector; and some level of fraud is to be expected because it is not reasonable to eliminate all fraud in its programs. The instances of fraud encountered by the Bank in recent years have centered on small exposures, according to bank managers. Thus, the current level of fraud

⁶⁸We selected this leading practice for review based on relevancy, following discussions with Bank managers, review of Bank documents, and results obtained from our employee survey.

⁶⁹[GAO-14-704G](#), 6.09.

⁷⁰According to *Standards for Internal Control in the Federal Government*, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. [GAO-14-704G](#), 6.08.

the Bank experiences is “defensible,” given the Bank’s mission and number of transactions it undertakes, according to the CRO. Bank managers said that fraud activity has steadily declined over the last decade, based on what they cited as fraud indicators that are reviewed by the Bank’s OGC.

Bank managers also pointed to claims as another indication of declining fraud activity. Transaction participants file claims for losses covered under Bank loan guarantee and insurance products, such as if a borrower fails to make required payments. The Bank considers fraud to be a subset of transactions that result in claims, and managers cited declining claims activity over the last decade as an indirect measure of fraud activity. Table 1 shows a history of claims paid for fiscal years 2008 through 2017.

Table 1: Claims Paid for Medium- and Short-Term Products, Export-Import Bank of the United States, Fiscal Years 2008–2017

| n/a | Dollars in millions |
|-------------|---------------------|
| Fiscal year | Total claims paid |
| 2008 | 109.8 |
| 2009 | 159.4 |
| 2010 | 145.1 |
| 2011 | 113.2 |
| 2012 | 36.7 |
| 2013 | 48.8 |
| 2014 | 40.3 |
| 2015 | 42.9 |
| 2016 | 32.5 |
| 2017 | 17.0 |

Source: Export-Import Bank of the United States. | GAO-18-492

Overall, Bank managers told us that in light of the decline in fraud they described, the task facing the Bank is to make sure that staff do not lose their focus on fraud and become too comfortable.

We asked the Bank to provide statistics supporting the claimed long-term decline in fraud activity, based on fraud indicators. In response, managers told us the indicators are actually not “precise or numerical measures.” Instead, OGC noted the office is aware of fraud activity through

“consultations and [a] general sense of day-to-day business.”⁷¹ As for claims, we note that not all fraud activity may result in claims. Consequently, an analysis of claims alone may not reveal a complete or accurate view of fraud activity. In addition, although Bank statistics we reviewed show a decline in number of claims filed from fiscal year 2014 through nearly the end of fiscal year 2017, the decline is likely attributable to the lapse in the Bank’s authority in fiscal year 2015, according to a Bank report.⁷²

While the Bank has adopted a general position on its fraud risk tolerance—that the current level of fraud is defensible, given the Bank’s mission—its current risk tolerances are not specific and measurable. Without more specific and measurable risk tolerances, the Bank cannot be assured of the extent to which any fraud risks exceed the Bank’s fraud risk tolerance. For example, a measurable risk tolerance could express willingness to tolerate an estimated amount of potentially fraudulent activity, given resource constraints in eliminating all fraud risks.

The Bank Will Revise Its Practices, According to Managers

After initially telling us that the Bank’s fraud risk management practices are working well and do not need modification, Bank managers later told us they will revise their approach. They now plan to conduct periodic fraud risk assessments and assess risks to determine a fraud risk profile, as provided in GAO’s Fraud Risk Framework, they said. Asked what prompted the changes, the CRO attributed them to our inquiries plus the Bank’s own growing experience with enterprise risk management. Bank managers also noted that since 2013, there has been an evolution in Bank antifraud controls, as part of what they refer to as a continuous improvement process.

⁷¹Until we inquired, the Bank did not track the number of referrals from OGC to the OIG. According to these newly prepared figures, referral activity has varied in recent years.

⁷²According to the Bank, the number of claims filed, by fiscal year, has been as follows:

| | |
|-------|----------------------------|
| 2014: | 176 |
| 2015: | 170 |
| 2016: | 132 |
| 2017: | 80 (through Aug. 2, 2017). |

Specifically, the Bank's new effort will include a range of new fraud management activities, according to the managers, starting with a fraud risk assessment and also including determining a fraud risk profile, on a priority-risk basis. The Bank also plans to identify residual risks and mitigating factors. In addition, according to the managers, this new work in addressing fraud risk is planned to include developing specific fraud risk tolerance or tolerances, with a metric for measuring such tolerance. As for implementation of the planned new approach, Bank managers stated they plan to complete a fraud risk assessment by December 2018 and to determine the Bank's fraud risk profile by February 2019.⁷³

However, Bank managers did not provide us with documentation describing in detail how they plan to ensure their fraud risk assessments and fraud risk profile are consistent with GAO's Fraud Risk Framework. For example, we requested documentation of any specific plans to adopt any of the four components of GAO's framework. Bank managers told us they plan to work with an outside consultant, and provided an outline of planned activities. However, the information did not describe how the Bank will ensure its risk assessments and profile include a full range of inherent fraud risks, including known fraud risks that are absent from its current risk register. Similarly, the managers did not provide documentation describing how the Bank's fraud risk assessments and profile will include risk tolerances that are specific and measurable.

Our employee survey results highlight the importance of the Bank's planned new approach. In comments, some respondents noted the changing nature of fraud, underscoring the importance of taking a wider, more proactive approach to fraud, which the Fraud Risk Framework encourages.

⁷³In making the changes Bank managers described to us, the Bank will reverse previous positions, according to our review. For example, Bank managers initially told us the Bank did not have a strategic or proactive system to assess, compile, weigh, or assign a value to any fraud risks to which the Bank may be exposed, and then prioritize appropriate control responses. Instead, the managers said they were confident that, based on previously identified fraud, if details in a transaction appear suspicious or inappropriate, the Bank was already familiar with the issue. In the case of prioritizing risk, the Bank had resisted that approach, out of concern it could encourage Bank staff to not scrutinize items if they appear to be lower priority, according to a Bank manager. As for setting risk tolerance, the manager previously said that because fraud at the Bank is now so low, it is not clear what would be gained by setting an acceptable level. Instead, the Bank's approach has been to monitor whether observed fraud activity shows an uptick.

Illustrative Comments from GAO's Survey of Bank Employees

- "There are tricks that financial fraudsters would use that many of our staff are unaware of."
- "The biggest risk is that we cease to see fraud controls as an ever-evolving process."
- "Types of fraud are constantly changing."
- "To assume that thieves don't evolve is inane, and to assume that you have the best, most evolved mechanisms for combating fraud is presumptuous."

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Given the importance, under a more proactive approach, of being able to identify and react to new forms of fraud, we also asked employees how well they believe Bank senior management understands new or changing ways of attempting or committing fraud. About two-thirds (67 percent) said senior Bank management understands "very well" or "for the most part," with the remaining respondents undecided or believing otherwise.⁷⁴

⁷⁴Remaining responses were understands "somewhat" (10 percent), "a little" (3 percent), "not at all" (1 percent), or "unsure/don't know" (19 percent).

The Bank Has Instituted Some Antifraud Controls but Not Developed a Strategy Based on a Fraud Risk Assessment, and Has Opportunities to Improve Fraud Awareness and Data Analytics

The Bank has instituted a number of antifraud controls but has not developed an antifraud strategy based on a fraud risk profile, or implemented specific control activities to achieve such a strategy. This is because, as discussed earlier, it has not yet completed a fraud risk assessment tailored to its operations. As described in the third component of GAO's Fraud Risk Framework, agencies should design and implement a strategy with specific control activities to address risks identified in the fraud risk assessment. We also found the Bank has opportunities to improve antifraud controls through greater fraud awareness and use of data analytics. Leading practices for fraud risk management under the third component include fraud awareness and data analytics activities, which can enhance the agency's ability to prevent and detect fraud.⁷⁵

Fraud Risk Framework Component 3:
Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation

⁷⁵The evaluation criteria here—strategy based on the fraud risk profile, and specific control activities arising from that—are the first two overarching concepts of the third component of GAO's Fraud Risk Framework. We selected the leading practices for review here based on relevancy, following discussions with Bank managers, review of Bank documents, and results obtained from our employee survey.



The Bank Has Instituted Some Antifraud Controls, but Has Not Developed an Antifraud Strategy in Accord with Leading Practices





The Bank currently employs a number of antifraud controls, both before and after transaction approval, which Bank managers told us include:

- Specific antifraud activities within individual business units, as they operate their respective programs.
- Review of transactions, including checking for fraud activity, following transaction approval.
- Later-stage review, such as examinations and recommendations by the Bank's OIG.

Preapproval antifraud efforts: Underwriting is the initial step in preventing fraud, and underwriters have a heightened awareness of fraud and irregularities, Bank managers told us. Under the Bank's antifraud procedures, underwriters in the business units should be aware of fraud risks in their transactions and be alert to indications of fraud. Prior to approval, transactions and their participants go through several evaluations. These can assist underwriters in preventing fraud, according to Bank procedures.⁷⁶ Figure 5 describes selected preapproval evaluations.

⁷⁶Many transactions are underwritten by Bank staff, managers told us. Some transactions—medium-term and working capital loan guarantees—rely on underwriting by outside lenders under delegated authority. Under such authority, the outside lenders act on the Bank's behalf, and their transactions receive the same guarantees as Bank-underwritten transactions. In such delegated transactions, the Bank relies on antifraud provisions imposed by the outside lenders' financial regulators. In addition, Bank managers told us these lenders also perform their own due diligence checks before authorizing funding.

Figure 5: Selected Export-Import Bank of the United States Evaluations Prior to Transaction Approval

| Type of evaluation | Description |
|---|---|
|  <p>Underwriting</p> | <p>This process—for evaluating the suitability of an application, including an assessment of transaction risk—is the Bank’s primary safeguard for preventing fraud, according to Bank managers and procedures. Various Bank programs are underwritten in different ways, and the details of underwriting may be transaction-specific.^a</p> |
|  <p>Database checks</p> | <p>Bank staff run the names of transaction participants against specialized databases, including sanction, watch, regulatory, and law-enforcement lists. The aim is to check whether transaction participants appear on any lists of prohibited or restricted parties maintained by the U.S. government and other entities.</p> |
|  <p>Enhanced due diligence</p> | <p>For selected transactions, the Bank performs “enhanced due diligence.” This includes Internet research, regional office visits, contact with the U.S. embassy, contact with the U.S. Department of State, third-party due diligence reports, and applicant site visits.</p> |
|  <p>“Red flag” indicators</p> | <p>Based on fraud experienced, the Bank has created a list of fraud “red flags”—warning indicators—to evaluate potential for fraud. Examples: altered or falsified documentation, multiple changes in the amount of financing requested, and discrepancies between key documents, such as tax statements and sales receipts.</p> |

Source: Export-Import Bank of the United States (the Bank). | GAO-18-492




^aAccording to Bank procedures: “In all Bank programs, the underwriters and loan officers (to the extent the loan officers are different than the underwriters), as well as [others who may be involved in processing the transaction] should be aware of the risks of fraud in their transactions, should be alert to indications of fraud, and should consider fraud risks in the course of underwriting.”

According to the Bank, additional preapproval measures include analyzing lenders, focusing on sufficiency of due diligence or what appear to be a high level of claims; requiring collateral on most medium-term transactions; not allowing online applications to proceed unless applicants provide required information; and using a two-step approval process, in which both the underwriter and the underwriter’s supervisor must approve certain transactions.

Postapproval antifraud efforts: Postapproval monitoring is generally not directed specifically at fraud, but plays a key role in fraud detection. Specifically, Bank managers told us that the Bank typically learns of fraud

through the claims process—that is, after transactions are approved.⁷⁷ Figure 6 describes postapproval monitoring.

Figure 6: Export-Import Bank of the United States Monitoring of Transactions after Approval

| Type of evaluation | Description |
|--|---|
|  <p>Claims</p> | <p>According to Bank officials, postapproval claims and collections matters are the primary way the Bank discovers fraud. Transaction parties file claims for losses, such as when a borrower defaults. After claims are filed and paid, the Bank seeks to collect on the losses, and investigate why a default took place.</p> |
|  <p>Compliance reviews</p> | <p>The Bank’s Credit Review and Compliance division examines a sample of transactions, to include reviewing items such as transaction documents and disbursement schedules, and contacting parties involved, such as exporters or suppliers. About 95 percent of these reviews are done on a random basis, with the remainder done on a “judgmental risk basis.”</p> |
|  <p>Ongoing monitoring</p> | <p>After transaction approval, two Bank units assume responsibility for ongoing monitoring.^a This includes monitoring of transaction participants’ financial performance, rerunning database checks on participants, making site visits, or verifying other terms and conditions of the Bank’s agreements. According to Bank officials, the goal is to stay ahead of developments that could jeopardize successful completion of transactions.</p> |

Source: Export-Import Bank of the United States (the Bank). | GAO-18-492

^aAccording to Bank managers, the Transportation Portfolio Management Division monitors transactions such as helicopters, corporate aircraft, and commercial jetliners. The Asset Management Division monitors nontransportation transactions, ranging from small working capital deals up to multi-billion-dollar projects, they also said.

Later, third parties, such as the Bank’s OIG, review transactions and operations, the chief risk officer told us. The Bank has developed a policy

⁷⁷Claims are paid after a default occurs. The Bank can seek to recover its payouts, but the recovery rate can be low, at least initially. In a recent report, the Bank reported gross defaults—which is total claims paid and overdue loans, and not solely for fraud—of \$571.3 million as of March 2018. Of that amount, the Bank reported recoveries of \$26.1 million, for a recovery rate of 4.6 percent. Over time, amounts recovered increase, Bank managers told us, with full recovery typically taking several years. After discussion with Bank managers and at their suggestion, we requested claims data to reflect earlier transactions. In response, the Bank in April 2018 examined claims paid from fiscal years 2009 to 2013, to determine recoveries made on those claims. According to the Bank, it paid \$602.2 million in claims for those years, and has recovered \$210.9 million, for a recovery rate of 35 percent. We specified the earlier period in order for several years to have elapsed since the claims were paid.

and expectations for employee conduct in matters of possible fraud, imposing a duty to report any “suspicion” of fraud to OGC or the OIG.⁷⁸ In particular, OGC is not selective about what information it passes to OIG, a manager told us—anything about Bank transactions is referred, no matter the strength of the evidence.

In our employee survey, some respondents expressed concern that there is reliance on postapproval monitoring, versus greater scrutiny at the time of application.

Illustrative Comments from GAO’s Survey of Bank Employees

- The current division of responsibilities “is not the most effective way for the Bank to oversee fraud and fraud risk, as responsibility needs to be given to the teams on the front end—such as the individual relationship managers and loan officers—not on the back end.”
- The current arrangement “seems to be more of an after-the-fact approach to potentially (if reluctantly) detecting fraud than any proactive encouragement to actively prevent fraud.”

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Although the Bank has instituted these pre- and postapproval antifraud controls, they may not provide the most effective protection available. According to GAO’s Fraud Risk Framework, the leading practice is for agencies to design and implement antifraud controls based on a strategy determined after performing a fraud risk assessment and creating a fraud risk profile. However, as previously discussed, the Bank has not yet completed such an assessment to determine such a profile. Consequently, the Bank cannot develop an antifraud strategy and associated controls that meet the leading practice until it has completed a fraud risk assessment and documented the results in a fraud risk profile.

As noted earlier, Bank managers told us they now recognize the need to conduct assessments and develop a fraud risk profile for the Bank, and that they plan to complete this work by February 2019. They further told us that, after conducting a risk assessment and developing a fraud risk profile, they plan to design and implement antifraud controls as may be indicated by the assessment, in keeping with the framework’s third component. Until the Bank creates an antifraud strategy based explicitly on a fraud risk assessment and corresponding fraud risk profile, and has

⁷⁸According to the Bank, all employee reports of suspected fraud made to OGC are passed along to the OIG, regardless of whether OGC concurs that a referral was warranted.

designed and implemented specific control activities to prevent and detect fraud, it is at risk of failing to address fraud vulnerabilities that could hurt its performance, undermine its reputation, or impair its ability to fulfill its mission.

The Bank Has Opportunities to Improve Fraud Awareness among Its Staff

As provided in GAO's Fraud Risk Framework, increasing awareness of potential fraud schemes can serve a preventive purpose, by helping to create a culture of integrity and compliance, as well as to enable staff to better detect potential fraud. The Bank currently takes some steps to share information on fraud risks across the institution, through a variety of mechanisms, but it has opportunities to further improve information sharing to build fraud awareness.

Training, cited earlier, is a leading practice of the Fraud Risk Framework, by which an agency can build fraud awareness.⁷⁹ In particular, the framework cites requiring that all employees, including managers, attend training when hired and then on an ongoing basis thereafter. As discussed earlier, the Bank now conducts some training, and Bank managers told us they see our survey results as an opportunity to provide additional training. By extending training requirements to all employees, the Bank can seek to build awareness as broadly as possible, and with that, further reinforce antifraud tone and culture. Currently, according to our assessment of information the Bank provided, it does not offer dedicated fraud training across the organization, for all employees and on an ongoing basis.

Another way to build fraud awareness is information sharing. For example, a manager in the Bank's OGC told us he monitors fraud activity and communicates relevant fraud-related information to other units in the Bank, based on considerations such as whether a situation could be repeated in other cases. However, there are limitations in information-sharing. For example, the Bank's OGC told us it restricts how widely it shares information on parties placed on an internally generated "watch list" of parties that should be scrutinized. The Bank also cannot share

⁷⁹We selected this leading practice for review based on relevancy, following discussions with Bank managers, review of Bank documents, and results obtained from our employee survey.

information provided by OIG on parties in a confidential law enforcement database as being under investigation, managers said, because those parties may not know they are under investigation. The reasons for such caution, according to managers, include the Privacy Act of 1974⁸⁰ and fear of creating a “de facto debarment list” absent any formal findings of fraud. In addition, CRC division managers told us that when the division discovers fraud-related information, it communicates such information to appropriate Bank staff.

Despite concerns, we found there are opportunities for greater compilation and sharing of information, and employees said in our survey that they believe wider sharing of fraud-related information would be beneficial to building fraud awareness and performing their duties. For example, one way of boosting fraud awareness would be if Bank managers comprehensively tracked referrals of suspected fraud matters to the OIG and shared case outcomes with Bank staff, Bank managers told us. However, Bank managers told us they do not currently maintain and share such information on cases of suspected fraud referred to the OIG.⁸¹ Relatedly, GAO’s Fraud Risk Framework notes the opportunity for an agency to collaborate with its OIG when planning or conducting training, and promoting the results of successful OIG investigations internally.

Some program managers also told us maintaining a repository of known fraud cases could aid in compliance and transaction approvals, but the Bank does not maintain and share this information with staff. In addition, as Bank managers acknowledge, compiling and maintaining information collected through the Bank’s database checks on transaction participants

⁸⁰See 5 U.S.C. § 552a. The act establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

⁸¹For OIG referrals, the Bank has used an informal record-keeping system maintained by OGC, a Bank manager said, which does not include all such referrals. For outcomes, OGC usually does not hear back from the OIG on dispositions, the manager said, and thus does not maintain such information. Bank managers also noted to us that years can elapse between when fraud is reported and a determination is made, undercutting the value of outcome information for current fraud controls. We note that while that may be true, it does not necessarily negate the value of all outcome-related information.

could serve as a library of useful information. However, Bank managers told us they do not currently maintain and share such information.⁸²

In our survey, we asked employees whether Bank management provides any information on outcomes of fraud cases involving the Bank or Bank staff. Nearly half of respondents (49 percent) said no. About a third (35 percent) said yes. Among a subset of employees who reported that their job duties include direct responsibility for fraud matters, the “Yes” figure was higher but still less than a majority (41 percent).⁸³ Some survey respondents noted lack of information-sharing about fraud practices and case outcomes, including that staff processing transactions must rely on personal memory for fraud issues that arose in previous transactions.

Illustrative Comments from GAO’s Survey of Bank Employees

- “In some cases, there is no way to track bad actors or suspected fraudsters unless someone working the new transaction remembers that there was an issue with the actor in a previous transaction.”
- “Management seems to not want to discuss any fraud with staff. Instead, they should use the opportunity to educate staff about fraud that occurs and show the consequences that result. They need to be more open.”
- “While the Bank has put a lot of best practices in place, more could be done to more regularly communicate to staff about changing practices in committing and detecting fraud.”
- “Outcomes are rarely relayed to staff.”

Source: GAO survey of non-senior-management Bank employees. | GAO-18-492

Underscoring the value of sharing information, our survey also found that when Bank management does share fraud-related information, Bank staff tend to find it useful in carrying out their duties. For those reporting that management does share fraud information, more than half of respondents (54 percent) said they found such information was “extremely” or “very” helpful in their job duties. Similarly, for those who reported they can readily access fraud-related information on their own from internal Bank

⁸²For the database queries, Bank managers told us they have broadly analyzed results of queries, to determine how much of the information is meaningful, but not gone further. Capturing database search information offers the opportunity to create data to improve underwriting, as well as for transaction data analytics generally, the managers said.

⁸³There were 153 Bank employees in this subset.

resources, nearly two-thirds (63 percent) said the information was “extremely” or “very” helpful.⁸⁴

In response to our inquiries, Bank managers said they plan to evaluate the feasibility of maintaining and sharing case outcome and database query information. In addition, they said OGC is exploring how it might share more fraud-related information, but in a protected way. In particular, the Bank wants to be able to share information on “integrity factors,” especially at the underwriting level. One way to do this might be distribution of fraud case studies as a refresher for staff, they said.

Until the Bank makes greater efforts to share information on known fraud schemes or bad actors, the Bank forgoes the opportunity, as described in the Fraud Risk Framework, to build staff awareness that could enhance antifraud efforts in these ways. For example, by not sharing the outcomes of suspected fraud matters referred to the OIG, the Bank forgoes the opportunity to build awareness through lessons learned from actual cases, which could give staff especially relevant insight into future attempts at fraud.

The Bank Has Opportunities to Improve Data Analytics to Fight Fraud

GAO’s Fraud Risk Framework cites data analytics as a leading practice for preventing and detecting fraud; in particular, to mitigate the likelihood and impact of fraud. We found the Bank makes limited use of data analytics for antifraud purposes. For example, it conducts analyses of claims cases, according to Bank managers, and, as noted earlier, considers fraud to be a subset of transactions that result in claims. Documentation of such activity provided to us by the Bank includes analyses and statistical summaries, such as number and types of claims filed, and tallies of claim decisions (for example, approved, denied).

⁸⁴In our survey, we also asked employees how frequently—other than through Bank-provided training—Bank management provides fraud- or fraud risk–related information that is directly applicable to their jobs. The results were mixed. About a third (34 percent) said Bank management “very frequently” or “fairly frequently” provides such information. About an equal number (32 percent) said management “occasionally” provides this information.

However, the Bank does not perform data analytics, which are additional leading practices described in the Fraud Risk Framework.⁸⁵

According to one manager, the Bank does not perform data analytics on its transaction-related data because the Bank OIG does not provide a specific transaction number (or “deal number”) necessary to link fraud cases it successfully pursues to the specific transactions from which the OIG action arises. Without that link, the Bank cannot distinguish transactions proven to be fraudulent from other, nonfraudulent transactions in its data, the Bank manager said. The link would be necessary for data-analytics purposes, the manager said. This inability to tie proven fraud cases to individual transactions, based on inability to obtain the key identifying information from the OIG, is a significant weakness in the Bank’s postapproval transaction monitoring, the manager further said.

The Bank and its OIG take different views on this linking information. The Bank has asked the OIG to provide these specific transaction numbers in an effort to link proven fraud cases to its transaction data, according to one Bank manager. OIG officials, meanwhile, told us they always notify the Bank when a conviction is made, and provide as much information as possible and appropriate under the circumstances, including company name and individual name. OIG officials also noted that, even without the specific transaction number the Bank requests, the Bank should nevertheless be able to use OIG-provided case data to search its own transaction files and successfully locate corresponding transactions.⁸⁶

In response to our inquiries, Bank managers said they are now considering a move into data analytics, including predictive analytics, to

⁸⁵According to GAO’s Fraud Risk Framework, data-analytics activities such as data mining (identifying suspicious activity or transactions, including anomalies, outliers, and other red flags, within data) or data matching (comparing information in one source to another, to identify inconsistencies) can allow agencies to prevent and detect fraud. Predictive analytics, meanwhile, can identify particular types of behavior, including fraud, before transactions are completed.

⁸⁶OIG officials also cautioned that making one-for-one matches to Bank transaction data may be difficult. For example, they said, there may be several transactions related to a fraud. However, the OIG may use only some of those transactions to prosecute a case, because they are the easiest to prove.

guard against fraud.⁸⁷ However, until the Bank has a feasible and cost-effective means of linking OIG cases to specific transactions, its ability to use data-analytics for antifraud purposes will be limited. Without the ability to make use of data-analytics, the Bank forgoes the opportunity to develop a best-practices antifraud tool that could aid in identifying potential fraud retrospectively, on transactions already approved, or prospectively, in advance of approval.

⁸⁷In particular, the Bank sees opportunities for more data analytics on fraud that develops postapproval, Bank managers said. Most fraud the Bank discovers is postauthorization, such as in shipping, they noted.

The Bank Has Opportunities to Improve Monitoring and Evaluating Outcomes of Its Fraud Risk Management Activities

The fourth and final component of GAO's Fraud Risk Framework calls for ongoing monitoring and periodic evaluations of the effectiveness of antifraud controls. This monitoring and evaluation should be from the specific perspective of antifraud controls established based on a comprehensive fraud risk assessment. Such activities can serve as an early warning system to help identify and resolve issues in fraud risk management—whether they involve current controls or prospective changes. Ongoing monitoring and periodic evaluations provide assurances to managers that they are effectively preventing, detecting, and responding to potential fraud. Further, according to the framework, effective monitoring and evaluation focuses on measuring outcomes and progress toward achieving objectives.⁸⁸

Fraud Risk Framework Component 4:
Evaluate outcomes using a risk-based approach and adapt activities to improve fraud risk management



Source: GAO. | GAO-18-492

Because the Bank has not completed a comprehensive fraud risk assessment, or designed antifraud controls based on such an assessment, it is not in a position to fulfill this final component. Even at that, however, we found the Bank does not generally evaluate the effectiveness or efficiency of its current fraud risk management practices. For example, OGC and CRC managers—who form the dedicated entity for managing fraud risks (as described earlier in component one)—both told us they are unaware of any procedure to periodically assess the effectiveness of the Bank's fraud risk management policies. In addition, the Bank currently has no formal method for tracking fraud activity, according to a Bank manager. Thus, the Bank is not in a position to explicitly judge the effectiveness of antifraud controls. Further, as described earlier, Bank managers told us the fraud indicators they do track are not precise or numerical measures and that, instead, OGC is aware of fraud activity through a general sense of daily business.

Following our inquiries, Bank managers told us they plan to revise their approach to monitoring, evaluating, and adapting their fraud risk

⁸⁸The fourth component of GAO's Fraud Risk Framework, with three overarching concepts, centers on evaluating outcomes of assessment-based fraud risk management activities, on a risk-based basis, and then adapting those activities as indicated to improve fraud risk management.

management practices. They said they now plan to evaluate the effectiveness of those practices, following adoption of the second and third components of GAO's Fraud Risk Framework, and with the intent to adapt controls as indicated necessary, in accordance with the framework's fourth component. Timing will depend on implementation of the underlying fraud risk assessment, Bank managers told us. The Bank cannot be assured that its antifraud controls are optimal until it has fulfilled component four of GAO's Fraud Risk Framework in the comprehensive fashion envisioned, following previous full implementation of components two and three. In particular, it cannot be assured that current practices are adequate, based on inherent program risks.

Conclusions

Proactively and strategically managing fraud risks can aid the Bank's mission of supporting American jobs by facilitating U.S. exports, by reducing not only the risk of financial loss to the government, but also the risk of serious reputational harm to the Bank. The Bank has taken some steps to address fraud that are among leading practices identified in GAO's Fraud Risk Framework. But overall, the Bank has approached fraud risk management on a fragmented, reactive basis, and its antifraud activities have not been marshalled into the kind of comprehensive, strategic fraud risk management regime envisioned by GAO's Fraud Risk Framework and its leading practices.

Chiefly, this is because the Bank has not anchored its fraud risk management policies in a comprehensive fraud risk assessment and corresponding risk profile, tailored to its operations, and then implemented controls designed to address the specific fraud risks identified in the assessment. Some fraud risk facing the Bank is already known, such as fabricated documentation. But as the Bank acknowledges, in addition to fraud risk inherent in its complex lines of business, it also faces significant risk from new or unfamiliar deal structures it may employ, and in new and unfamiliar technologies and industries it may service, where it has limited experience. Regular, comprehensive fraud risk assessments will address not only known types of fraud, but also seek to identify where fraud can occur and the types of fraud the program faces, including likelihood and impact.

Accordingly, until the Bank begins conducting thorough, systematic assessments of its fraud risks, and compiles a risk profile prioritizing such risks, it cannot be assured that it satisfactorily understands its

vulnerabilities to fraud and any gaps in its capabilities for addressing them. Following on from that, without developing and implementing an antifraud strategy that builds on the findings of the comprehensive risk assessments and risk profile, the Bank cannot be assured that its antifraud control activities are optimally designed for, and targeted to, the actual fraud risks its faces—meaning that it could be failing to address significant risks or targeting the wrong ones. Finally, without establishing outcome-oriented metrics and then regularly reviewing progress toward meeting these goals, the Bank cannot be assured that its antifraud control activities are working as intended.

As we concluded our review, the Bank, encouragingly, said it would adopt the more proactive approach described by GAO's Fraud Risk Framework. Thus, the Bank now needs to follow through on its stated intent to change its practices, and accomplish the tasks, described to us by Bank managers, as intended and in a timely fashion. This is true not only for current operations, but also prospectively, for the large transaction backlog the Bank faces, which Bank managers will process if or when the Bank's quorum issue is resolved, and which could stress Bank fraud controls.

The Bank's identification of a dedicated entity to lead fraud risk management activities can be an important step in the right direction if that move now becomes the start of a sustained commitment. By fully adopting the elements of the framework, the Bank can strengthen its antifraud culture, better understand fraud risks facing its products and programs, and reshape how it monitors and evaluates the outcomes of its fraud risk management activities. In doing so, it will be better positioned to protect taxpayers and its multi-billion-dollar portfolio, while still meeting its mission to support American jobs and exports.

Even though Bank managers have already told us they plan to implement the framework, they did not provide us documentation describing in detail how they will ensure their fraud risk assessment and fraud risk profile are consistent with leading practices of the framework—such as by ensuring the risk assessment considers all inherent fraud risks and the risk profile reflects risk tolerances that are specific and measurable. Thus, we include the following framework-specific recommendations in order to comprehensively enumerate relevant issues we identified, as well as to present clear benchmarks of accountability for assessing Bank progress. This complete listing is important in light of the Bank's recent embrace of the framework; changes in the Bank's executive leadership and

vacancies on the Bank Board; and expected congressional consideration of the Bank's reauthorization in 2019.

Recommendations for Executive Action

We are making the following seven recommendations to the Bank:

The acting Bank president and Board chairman should ensure that the Bank evaluates and implements methods to further promote and sustain an antifraud tone that permeates the Bank's organizational culture, as described in GAO's Fraud Risk Framework. This should include consideration of requiring training on fraud risks relevant to Bank programs, for new employees and all employees on an ongoing basis, with the training to include identifying roles and responsibilities in fraud risk management activities across the Bank. (Recommendation 1)

As the agency begins efforts to plan and conduct regular fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that the Bank's risk assessments and profile address not only known methods of fraud, including those that are absent from its current risk register, but other inherent fraud risks as well. (Recommendation 2)

As the agency begins efforts to plan and conduct regular fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that the risk profile includes risk tolerances that are specific and measurable. (Recommendation 3)

The acting Bank president and Board chairman should ensure that the Bank develops and implements an antifraud strategy with specific control activities, based upon the results of fraud risk assessments and a corresponding fraud risk profile, as provided in GAO's Fraud Risk Framework. (Recommendation 4)

The acting Bank president and Board chairman should ensure that the Bank identifies, and then implements, the best options for sharing more fraud-related information—including details of fraud case referrals and outcomes—among Bank staff, to help build fraud awareness, as described in GAO's Fraud Risk Framework. (Recommendation 5)

The acting Bank president and Board chairman should lead efforts to collaborate with the Bank's OIG to identify a feasible, cost-effective means to systematically track outcomes of fraud referrals from the Bank to the OIG, including creating a means to link the OIG's proven cases of fraud to the specific Bank transactions from which the OIG actions arose.

If any such means are found to be feasible and cost-effective, the acting Bank president and Board chairman should direct appropriate staff to implement them, with such information to be used for purposes consistent with GAO's Fraud Risk Framework, such as data analytics. (Recommendation 6)

The acting Bank president and Board chairman should ensure that the Bank monitors and evaluates outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and that it subsequently adapts antifraud activities or implements new ones, as determined to be appropriate and consistent with GAO's Fraud Risk Framework. (Recommendation 7)

Agency Comments and Our Evaluation

We provided a draft of this report to the Bank for review and comment. In written comments, summarized below and reproduced in appendix III, the Bank agreed with our recommendations. The bank also provided technical comments, which we incorporated as appropriate.

In its written comments, the Bank said it will take several steps to implement our recommendations to improve its fraud risk management activities. For example, the Bank stated it would continue to evaluate and implement methods to promote and sustain an antifraud tone that permeates the Bank's organizational culture. In assessing fraud risks, the Bank stated it will include not only known risks, but also other inherent risks not yet known to have led to fraud. Following a fraud risk assessment as provided in GAO's Fraud Risk Framework, the Bank stated that it will develop antifraud controls based on that assessment, subject to cost-benefit analysis. The Bank also stated that it will monitor and evaluate outcomes of its fraud risk management activities, and adapt existing controls or implement new controls as indicated, subject to cost-benefit analysis. The Bank further stated it will identify and implement ways to share more fraud-related information.

In its written comments, the Bank also raised four concerns about our work.

First, the Bank stated that it keeps substantial reserves for losses, which protect against taxpayer costs. We clarified our report to indicate that Bank officials told us they maintain reserves to protect against taxpayer costs. We did not evaluate the extent to which these reserves protect

against taxpayer costs because doing so was outside the scope of our review.

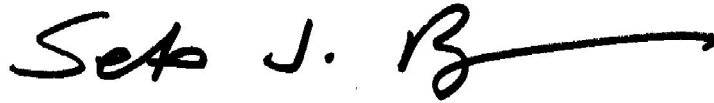
Second, the Bank stated our employee survey does not directly support some of the conclusions that we draw from responses received, and that only 24 percent of respondents were in the Export Finance area, which handles underwriting of Bank transactions. We note that the leading practices of the Fraud Risk Framework call for involving all levels of the agency in setting an antifraud tone that permeates the organizational culture. We also note that the Office of the Export Finance is not the only division involved in fraud control activities. For example, during our review, Bank managers told us that employees in the Credit Review and Compliance division, the Office of the General Counsel, and the Office of the Chief Financial Officer, among other offices, are also involved in fraud control activities. Thus, we believe it is appropriate that survey responses from those who work in these and other offices are included in our survey results. As noted in our report, Bank managers, in interviews, and staff, in our employee survey, generally expressed positive views of the Bank's antifraud culture, but they hold different views on key aspects of that culture. We believe that our survey results support these findings, as well as related conclusions and recommendation (Recommendation 1), with which the Bank agreed.

Third, the Bank stated that it has been very effective in preventing, detecting, and prosecuting fraud in Bank transactions. Our review evaluated the extent to which the Bank has adopted leading practices for managing fraud risks, as described in the Fraud Risk Framework. We did not evaluate the operational effectiveness of specific Bank control activities for preventing, detecting, and prosecuting fraud because doing so was beyond the scope of our review.

Fourth, the Bank stated that our report and the employee survey did not clearly and consistently distinguish between fraud and fraud risk, which may lead to confusion in both the survey responses and the analysis in the report. However, we define the terms "actual fraud" and "fraud risk" in our employee survey, which appears in appendix II. Further, as described in greater detail in appendix I, we pretested and modified the survey to ensure questions were understood by respondents and that we used correct terminology. This process allowed us to determine whether survey questions and answer choices were clear and appropriate. Thus, we believe the survey results support our findings. Overall, as noted, these findings include positive views of the Bank's antifraud culture as well as differing views on some aspects of that culture.

We are sending copies of this report to the appropriate congressional committees, the acting president and Board chairman of the Bank, and other interested parties. In addition, the report is available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staffs have any questions about this report, please contact me at (202) 512-6722 or bagdoyans@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made key contributions to this report are listed in appendix IV.

A handwritten signature in black ink that reads "Seto J. Bagdoyan". The signature is written in a cursive style with a long horizontal stroke extending to the right from the end of the name.

Seto J. Bagdoyan
Director of Audits
Forensic Audits and Investigative Service

List of Committees

The Honorable Mike Crapo
Chairman
The Honorable Sherrod Brown
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Jeb Hensarling
Chairman
The Honorable Maxine Waters
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Lindsey Graham
Chairman
The Honorable Patrick Leahy
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
United States Senate

The Honorable Hal Rogers
Chairman
The Honorable Nita Lowey
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report examines management by the Export-Import Bank of the United States (the Bank) of fraud risks in its export credit activities, by evaluating the extent to which the Bank has adopted the four components described in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework).¹ Specifically, we evaluate the extent to which the Bank has

- established an organizational culture and structure conducive to fraud-risk management;
- planned regular fraud risk assessments and assessed risks to determine a fraud risk profile;
- designed and implemented a strategy with specific control activities to mitigate assessed fraud risks; and
- evaluated outcomes using a risk-based approach and adapted activities to improve fraud risk management.

To examine the extent to which the Bank has adopted the components of GAO's Fraud Risk Framework, we reviewed Bank policy and governance documentation, plus other documentation; reviewed GAO and Bank Office of the Inspector General reports on fraud and fraud risk management topics; reviewed relevant reports of the Congressional Research Service and the Congressional Budget Office; and reviewed

¹GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 2015).

other reports and background information.² Documentation we reviewed included Bank operating procedures, details of database search procedures, Bank annual reports, reports to Congress, the Bank's strategic plan, risk assessments, and other materials.

We also interviewed a range of Bank managers, at both the senior-management level and those overseeing relevant Bank operating units. These included the Bank's chief financial officer, its chief risk officer, its acting chief operating officer, those with specific antifraud responsibilities, and others responsible for individual business units. These individual business units included those with responsibilities for monitoring transactions following approval.

We then assessed our findings on the Bank's fraud risk management practices and its antifraud controls against provisions of the Fraud Risk Framework, which also incorporates concepts from GAO's *Standards for Internal Control in the Federal Government*.³

Survey Development and Administration

To examine the extent to which the Bank has established an organizational culture and structure conducive to fraud risk management, we conducted a web-based survey of Bank employees. In our survey, we assessed, among other things, perceptions of the Bank's organizational culture and attitudes toward fraud and fraud risk management, and

²See, for example, GAO, *Export-Import Bank: Enhancements Needed in Loan Guarantee Underwriting Procedures and for Documenting Fraud Processes*, [GAO-14-574](#) (Washington, D.C.: Sept. 9, 2014); GAO, *Enterprise Risk Management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk*, [GAO-17-63](#) (Washington, D.C.: Dec. 1, 2016); Office of the Inspector General, Export-Import Bank of the United States, *Evaluation of Risk Management Procedures and Chief Risk Officer Responsibilities*, OIG-EV-17-01 (Dec. 2, 2016); Office of the Inspector General, Export-Import Bank of the United States, *Audit of the Export-Import Bank of the United States Fiscal Year 2016 Financial Statements*, OIG-AR-17-01 (Nov. 15, 2016); Congressional Research Service, *Ex-Im Bank: No Quorum, No Problem?* IN10574 (Sept. 19, 2016); Congressional Research Service, *Export-Import Bank: Frequently Asked Questions*, R43671 (Apr. 13, 2016); Congressional Budget Office, *Estimates of the Cost of the Credit Programs of the Export-Import Bank* (June 25, 2014); Congressional Budget Office, *Answers to Questions for the Record Following a Hearing on the Export-Import Bank Conducted by the House Committee on Financial Services* (Oct. 6, 2014).

³GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014); commonly known as the "Green Book."

whether employees viewed senior Bank management as committed to establishing and maintaining an antifraud culture. We surveyed all non-senior-management Bank employees, regardless of their position or length of employment, who are responsible for implementing, but not determining, Bank policy (that is, those below the level of senior vice president).⁴ There were 403 employees in our survey population, and we received 296 responses, thus producing a response rate of 73.5 percent. We received sufficient representation across Bank offices and divisions, and, overall, obtained a range of employee views.

To develop our survey instrument, we utilized background research, leading practices as identified in GAO's Fraud Risk Framework, interviews with Bank senior managers, and other sources. We conducted in-person pretests of survey questions with five Bank employees, varying in position, Bank office or division, and seniority, at Bank headquarters in Washington, D.C. We pretested the survey instrument to ensure the questions were understood by respondents, that we used correct terminology, and that the survey was not burdensome to complete. This process allowed us to determine whether the survey question and answer choices were clear and appropriate. We modified our survey instrument as appropriate based on pretest results and suggestions made by an independent survey specialist. The final survey instrument included closed- and open-ended questions on Bank management and tone-at-the-top; fraud-related training and information; antifraud environment; and personal experiences with fraud at the Bank. Throughout the survey instrument, we defined important terms, such as "senior management," so respondents could interpret key concepts consistently through the survey.⁵

We administered the survey, via the World Wide Web, from July 31, 2017, through September 22, 2017. To do so, we obtained from Bank management a file of Bank employees with relevant identifying

⁴Based on these criteria, we eliminated the following positions (as listed in a file of all employees we obtained from the Bank) from our survey population: (1) senior vice president (SVP); (2) SVP of small business; (3) SVP and general counsel; (4) president and chairman; (5) SVP, chief of staff, and White House liaison; (6) SVP for communications; (7) SVP and chief financial officer; (8) chief information officer; (9) chief risk officer and SVP; and (10) SVP of business and product development.

⁵To see definitions used, see the survey instrument as presented to respondents, reproduced in app. II. Full responses to open-ended questions are not presented in this report, in order to protect respondent anonymity.

information. Before we opened the survey, the Bank president, at our suggestion, sent an email to employees notifying them of the forthcoming survey and encouraging them to respond. We also sent Bank employees a notification email describing the forthcoming survey, in advance of sending employees another email providing a unique username and password to access the web-based survey. To improve the response rate, we contacted Bank employees by phone who had not yet completed the survey (nonrespondents), to determine their eligibility, update their contact information, answer any questions or concerns about the survey, and seek their commitment to participate. We also sent multiple follow-up emails to nonrespondents encouraging them to respond, and provided instructions for taking the survey. These follow-up contacts reduced the possibility of nonresponse error. We sent our follow-up reminder emails to the survey population on August 10, 17, and 29, 2017, and September 1 and 14, 2017.

Because we surveyed all non-senior-management employees, the survey did not involve sampling error. To minimize nonsampling errors, and to enhance data quality, we employed recognized survey design practices in the development of the survey instrument and in the collection, processing, and analysis of the survey data. We calculated frequencies for closed-ended responses and reviewed open-ended response for themes and illustrative examples. When we analyzed the survey data, an independent analyst checked statistical programs used to collect and process responses. We selected survey excerpts—tallies of answers to selected questions, plus individual comments received from respondents—presented in the main text of this report based on relevance to the respective subject matter.

We conducted our performance audit from October 2016 to July 2018, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Appendix II: Results of GAO Survey of Bank Employees: “Anti-Fraud Controls at the Export-Import Bank of the United States”

As described in appendix I, GAO conducted a survey of employees of the Export-Import Bank of the United States (the Bank), to obtain their views on the Bank’s organizational culture and attitudes toward fraud and fraud risk management. We surveyed 403 employees and obtained 296 responses, for a response rate of 73.5 percent. Our survey did not rely on a sample, as we distributed it to the entire employee population identified. Although originally presented through the World Wide Web, the questions and answer choices that follow are the same wording as shown to Bank employees. Results are tallied for each question.¹ We omit, however, all individual responses to open-ended questions, in order to protect respondent anonymity. Underlined items indicate terms for which hyperlinked definitions were available in the original survey form.

¹“Valid responses” shown for each question refers to the number of survey respondents who answered that question. The number of valid responses may vary by question. Percentage totals for questions following may not add up to 100 percent due to rounding.

Please use these definitions when thinking about your answers—

- **"Fraud" generally means obtaining something of value through willful misrepresentation; and in particular, misconduct involving Bank transactions.**
- **We mean it to include actual fraud, as found through the judicial system or an administrative process; as well as "fraud risk" – an opportunity, situation, or vulnerability that could allow for someone to engage in fraudulent activity.**

In addition, fraud, or fraud risk, may be—

- **External in nature (such as fraudulent representations by Bank customers) or**
- **Internal in nature (such as employee conduct in dealing with customer transactions).**

General Questions

1. How long have you been employed at the Bank?

- Less than 1 year **10.8%**
- 1 year – 5 years **29.1%**
- More than 5 years **60.1%**

Valid responses: 296

2. Do your personal job duties include any direct responsibility for preventing, detecting, or otherwise addressing fraud or fraud risk?

- Yes **51.7%**
- No **40.5%**
- Unsure/don't know **7.8%**

Valid responses: 296

3. Please select the Office your division or department fits into.

| | |
|---|--------------|
| • Office of the General Counsel | 7.8% |
| • Office of Innovation and Performance | 5.7% |
| • Office of Information Management and Technology | 5.4% |
| • Office of the Export Finance | 24.0% |
| • Office of the Chief Financial Officer | 21.3% |
| • Office of the Senior Vice President Resource Management | 7.1% |
| • Office of Risk Management | 10.1% |
| • Office of the Senior Vice President Congressional Affairs | 1.7% |
| • Office of the Senior Vice President Communications | 1.0% |
| • Office of Policy Analysis and International Relations | 3.0% |
| • Office of the Senior Vice President Small Business | 8.1% |
| • Other | 4.7% |

Valid responses: 296

Management and Tone-at-the-Top

For this section and elsewhere, two additional definitions—

- *“Senior management” refers to Bank managers at the senior vice president level and above.*
- *“Management in general” refers to a broader management group – first-level supervisors and above.*

4. In your view, to what extent has Bank management in general established a clear anti-fraud tone for the Bank?

| | |
|---------------------|--------------|
| • A great deal | 50.3% |
| • A lot | 29.4% |
| • Some | 10.8% |
| • A little | 2.7% |
| • Not at all | 1.4% |
| • Unsure/don't know | 5.4% |

Valid responses: 296

-
5. Based on the actions of Bank senior management in particular, how important do you think preventing, detecting, and otherwise addressing fraud is to the Bank?
- Extremely important **61.5%**
 - Very important **25.0%**
 - Somewhat important **7.1%**
 - Slightly important **1.7%**
 - Not at all important **1.0%**
 - Unsure/don't know **3.7%**
- Valid responses: 296
6. Based on the actions of the managers of *your division* in particular, how important do you think preventing, detecting, and otherwise addressing fraud is to the Bank?
- Extremely important **60.5%**
 - Very important **27.9%**
 - Somewhat important **5.1%**
 - Slightly important **1.7%**
 - Not at all important **1.4%**
 - Unsure/don't know **3.4%**
- Valid responses: 294
7. How clearly has Bank management in general communicated a standard of conduct that applies to all employees, and which includes the Bank's expectations of behavior concerning fraud?
- Extremely clearly **44.6%**
 - Very clearly **33.3%**
 - Somewhat clearly **16.0%**
 - Slightly clearly **1.7%**
 - Not at all clear **1.7%**
 - Unsure/don't know **2.7%**
- Valid responses: 294

**Appendix II: Results of GAO Survey of Bank
Employees: “Anti-Fraud Controls at the
Export-Import Bank of the United States”**

1. Based on your experience, for each entity below, which category best describes the *level of responsibility* the entity has for overseeing fraud risk management activities at the Bank?

| | A great deal of responsibility | A lot of responsibility | Some responsibility | Little responsibility | No responsibility at all | Unsure/don't know | Valid responses |
|---------------------------------|---------------------------------------|--------------------------------|----------------------------|------------------------------|---------------------------------|--------------------------|------------------------|
| Office of General Counsel | 64.3% | 20.8% | 7.8% | 1.0% | 0.3% | 5.8% | 294 |
| Office of the Inspector General | 73.5% | 13.5% | 4.5% | 1.7% | 0.7% | 6.2% | 290 |
| Office of Risk Management | 57.1% | 22.5% | 8.2% | 1.4% | 0.7% | 10.2% | 294 |
| Bank senior management | 52.7% | 28.9% | 11.2% | 1.0% | 1.0% | 5.1% | 294 |
| All bank staff and managers | 40.3% | 32.4% | 20.5% | 1.7% | 0.7% | 4.4% | 293 |
| Other | 14.9% | 10.9% | 9.4% | 2.0% | 1.5% | 61.4% | 202 |

2. Thinking about your response to question 8, do you believe your answer represents the most effective way for the Bank to oversee fraud and fraud risk?

- Yes **62.4%**
- No **7.1%**
- Unsure/don't know **30.5%**

Valid responses: 295

9(a). [For all those not selecting “Unsure/don't know”] Why, or why not, is this the most effective way for the Bank to oversee fraud and fraud risk?

[Individual responses omitted.]

Fraud-Related Training and Information

3. Within the past two years, have you received fraud- or fraud risk-related training provided by the Bank (meaning conducted by the Bank directly, or otherwise arranged or sponsored by the Bank for employees)?

- Yes **65.8%**
- No **22.4%**
- Unsure/don't know **11.9%**

Valid responses: 295

10(a). If Yes, in your view, how relevant was this training to your job duties?

| | |
|-----------------------|--------------|
| • Extremely relevant | 33.2% |
| • Very relevant | 41.5% |
| • Somewhat relevant | 23.3% |
| • Slightly relevant | 1.6% |
| • Not at all relevant | 0.5% |
| • Unsure/don't know | — |

Valid responses: 193

10(b). If Yes, in your view, how useful was this training in aiding you in carrying out your job duties?

| | |
|---------------------|--------------|
| • Extremely useful | 28.0% |
| • Very useful | 35.2% |
| • Somewhat useful | 28.5% |
| • Slightly useful | 5.7% |
| • Not at all useful | 2.1% |
| • Unsure/don't know | 0.5% |

Valid responses: 193

4. Other than through training provided by the Bank, how frequently does Bank management in general provide you with information on fraud or fraud risk that directly applies to your job duties?

| | |
|--|--------------|
| • Very frequently | 11.5% |
| • Fairly frequently | 23.0% |
| • Occasionally | 32.1% |
| • Rarely | 15.9% |
| • Never | 4.7% |
| • Unsure/don't know | 4.1% |
| • Not applicable to my job or experience | 8.8% |

Valid responses: 296

11(a). [For those selecting in the range from Very frequently to Rarely] In your view, how helpful was the fraud- or fraud risk-related information from Bank management in carrying out your job duties?

| | |
|----------------------|--------------|
| • Extremely helpful | 20.7% |
| • Very helpful | 33.1% |
| • Somewhat helpful | 33.1% |
| • Slightly helpful | 5.8% |
| • Not at all helpful | 0.8% |
| • Unsure/don't know | 6.6% |

Valid responses: 242

5. How readily can you access on your own fraud- or fraud risk-related information from internal Bank resources (for example, the Bank's intranet) that directly applies to your job duties?

- Extremely readily **15.7%**
- Very readily **29.3%**
- Somewhat readily **16.7%**
- Slightly readily **5.8%**
- Not at all readily **4.8%**
- Unsure/don't know **16.3%**
- Not applicable to my job or experience **11.6%**

Valid responses: 294

12(a) [For those selecting in the range from Extremely readily to Slightly readily] In your view, how helpful was the fraud- or fraud risk-related information in carrying out your job duties?

- Extremely helpful **23.0%**
- Very helpful **40.3%**
- Somewhat helpful **26.5%**
- Slightly helpful **5.1%**
- Not at all helpful **1.0%**
- Unsure/don't know **4.1%**

Valid responses: 196

6. To what extent has fraud- or fraud risk-related information you've received from Bank management in general, or obtained through any other Bank resources, increased your understanding of fraud?

- A great deal **21.0%**
- A lot **31.4%**
- Some **24.7%**
- A little **6.8%**
- Not at all **5.7%**
- Unsure/don't know **4.7%**
- Not applicable to my job or experience **5.7%**

Valid responses: 296

[For question 14, we also tallied results for a subgroup of employees who said in response to question 2 that their job duties include direct responsibility for fraud matters.]

7. Do you receive from Bank management in general any information, through whatever sources, about the outcomes of fraud cases involving the Bank or Bank staff?
- Yes **35.3%**
 - No **48.8%**
 - Unsure/don't know **15.9%**
- Valid responses: 295

For employees who reported their "personal job duties include any direct responsibility for preventing, detecting, or otherwise addressing fraud or fraud risk"—

- Yes **41.2%**
 - No **44.4%**
 - Unsure/don't know **14.4%**
- Valid responses: 153

Antifraud Environment

8. In your view, how supportive is your workplace in preventing, detecting, or otherwise addressing fraud or suspected fraud at the Bank?
- Extremely supportive **42.5%**
 - Very supportive **36.3%**
 - Somewhat supportive **11.3%**
 - Slightly supportive **1.7%**
 - Not at all supportive **1.0%**
 - Unsure/don't know **7.2%**
- Valid responses: 292

9. How much confidence do you have in Bank senior management to respond to fraud or suspected fraud cases on a timely and appropriate basis?
- A great deal **48.1%**
 - A lot **28.1%**
 - Some **12.5%**
 - A little **4.1%**
 - Not at all **1.4%**
 - Unsure/don't know **5.8%**
- Valid responses: 295

10. How much confidence do you have in your peers in your division to respond to fraud or suspected fraud cases on a timely and appropriate basis?

- A great deal **50.2%**
- A lot **31.9%**
- Some **9.2%**
- A little **3.1%**
- Not at all **1.0%**
- Unsure/don't know **4.8%**

Valid responses: 295

11. How much confidence do you have in the managers in your division to respond to fraud or suspected fraud cases on a timely and appropriate basis?

- A great deal **57.1%**
- A lot **28.4%**
- Some **7.8%**
- A little **2.7%**
- Not at all **1.0%**
- Unsure/don't know **3.0%**

Valid responses: 296

12. How comfortable or uncomfortable would you feel raising concerns about fraud or suspected fraud at the Bank to appropriate managers?

- Very comfortable **70.2%**
- Somewhat comfortable **13.9%**
- Neutral – neither comfortable nor uncomfortable **10.5%**
- Somewhat uncomfortable **1.4%**
- Very uncomfortable **2.0%**
- Unsure/don't know **2.0%**

Valid responses: 295

13. In your view, how strong is the Bank's antifraud organizational culture?

- Extremely strong **34.6%**
- Very strong **35.3%**
- Somewhat strong **13.6%**
- Slightly strong **2.7%**
- Neutral – neither strong nor weak **–**
- Not at all strong **1.7%**
- Unsure/don't know **12.2%**

Valid responses: 295

14. Based on your overall knowledge and experience, how significant a risk is fraud to the Bank?

- Very significant risk **22.6%**
- Significant risk **25.0%**
- Some risk **25.7%**
- Slight risk **15.9%**
- No risk **1.4%**
- Unsure/don't know **9.5%**

Valid responses: 296

15. In your opinion, how well do you think Bank senior management understands new or changing ways of attempting or committing fraud against the Bank?

- Understands very well **34.9%**
- Understands for the most part **31.9%**
- Understands somewhat **9.5%**
- Understands a little **3.1%**
- Understands not at all **1.4%**
- Unsure/don't know **19.3%**

Valid responses: 295

16. In your view, should the Bank be more, or less, active in preventing, detecting, and otherwise addressing fraud or fraud risk?

- Much more active **9.8%**
- Somewhat more active **25.7%**
- Remain the same **43.6%**
- Somewhat less active **1.7%**
- Much less active **-**
- Unsure/don't know **19.3%**

Valid responses: 296

23(a). [For those not selecting "Unsure/don't know"] Why do you feel this is the appropriate level of activity for addressing fraud or fraud risk?

[Individual responses omitted.]

Priority and Employee Feedback

17. Among all the various activities of the Bank, where do you think preventing, detecting, and otherwise addressing fraud ranks as a priority overall?

- The top priority **18.0%**
- Among the top two or three priorities **52.9%**
- Mid-level priority **18.0%**
- Low priority **2.7%**
- Unsure/don't know **8.5%**

Valid responses: 295

18. How confident are you that Bank management in general would be receptive to employee ideas and suggestions on fraud- or fraud risk-related matters?

- Extremely confident **31.4%**
- Very confident **34.5%**
- Somewhat confident **17.6%**
- Slightly confident **5.1%**
- Not at all confident **4.4%**
- Unsure/don't know **7.1%**

Valid responses: 296

Personal Experiences

19. During your time at the Bank, while holding any position, have you ever personally been involved in a matter or transaction where fraud was investigated or later proven?

- Yes **18.5%**
- No **74.0%**
- Unsure/don't know **7.5%**

Valid responses: 292

26(a). [If Yes] Please describe the matter or transaction and the outcome.

[Individual responses omitted.]

20. In the past year, have you personally raised or reported concerns to any manager about a fraud- or fraud risk-related matter, or made a suggestion to improve anti-fraud controls?

- Yes **8.8%**
- No **88.5%**
- Unsure/don't know **2.7%**

Valid responses: 296

27(a). [If Yes] What issue(s) did you raise and what was the outcome?

[Individual responses omitted.]

[For questions 28–30, we tallied results to both include and exclude responses from those answering, "Not applicable to my job or experience."]

21. Based on your experience at the Bank, does the application process for long-term products provide enough time for Bank staff to conduct thorough due diligence on potential fraud risks?

- Always enough time **20.3%**
- Usually enough time **16.6%**
- Sometimes enough time **2.7%**
- Seldom enough time **–**
- Never enough time **0.3%**
- Unsure/don't know **20.3%**
- Not applicable to my job or experience **39.9%**

Valid responses: 296

Excluding "Not applicable to my job or experience"—

- Always enough time **33.7%**
- Usually enough time **27.5%**
- Sometimes enough time **4.5%**
- Seldom enough time **–**
- Never enough time **0.6%**
- Unsure/don't know **33.7%**

Valid responses: 178

22. Based on your experience at the Bank, does the application process for medium-term products provide enough time for Bank staff to conduct thorough due diligence on potential fraud risks?

- Always enough time **13.7%**
- Usually enough time **18.4%**
- Sometimes enough time **4.8%**
- Seldom enough time **0.7%**
- Never enough time **0.7%**
- Unsure/don't know **19.1%**
- Not applicable to my job or experience **42.7%**

Valid responses: 293

Excluding "Not applicable to my job or experience"—

- Always enough time **23.8%**
- Usually enough time **32.1%**
- Sometimes enough time **8.3%**
- Seldom enough time **1.2%**
- Never enough time **1.2%**
- Unsure/don't know **33.3%**

Valid responses: 168

23. Based on your experience at the Bank, does the application process for short-term products provide enough time for Bank staff to conduct thorough due diligence on potential fraud risks?

- Always enough time **8.8%**
- Usually enough time **18.9%**
- Sometimes enough time **8.5%**
- Seldom enough time **2.7%**
- Never enough time **0.7%**
- Unsure/don't know **19.3%**
- Not applicable to my job or experience **41.2%**

Valid responses: 296

Excluding "Not applicable to my job or experience"—

- Always enough time **14.9%**
- Usually enough time **32.2%**
- Sometimes enough time **14.4%**
- Seldom enough time **4.6%**
- Never enough time **1.1%**
- Unsure/don't know **32.8%**

Valid responses: 174

Conclusion

24. If you have additional comments on any of the items above, or on fraud- or fraud risk-related issues at the Bank generally, please feel free to provide them below.

[Individual responses omitted.]

25. Would you be willing to speak with GAO regarding your answers to the survey, the topics raised above, or other fraud-related matters?

- Yes **22.8%**
- No **77.2%**

Valid responses: 289

32(a). [If Yes] Please provide your name and contact information.

[Individual responses omitted.]

Appendix III: Comments from the Export-Import Bank of the United States

**Appendix III: Comments from the Export-
Import Bank of the United States**



Reducing Risk. Unleashing Opportunity.

June 29, 2018

Seto J. Bagdoyan,
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G St. NW
Washington, D.C. 20584

Dear Mr. Bagdoyan:

Thank you for providing the Export-Import Bank of the United States ("EXIM" or the "Bank") with the Government Accountability Office (GAO) draft report, "The Bank Needs to Continue to Improve Fraud Risk Management" (July 2018). The Bank supports the GAO's work and audits which complement the Bank's efforts to continuously improve its practices and procedures. EXIM Bank is proud of its cooperative relationship with GAO.

As highlighted in the General Comments A – D in the Omissions and Errata List response from EXIM to the GAO, there are several chief concerns EXIM would like to raise with the Report findings. First and foremost, EXIM keeps substantial reserves for losses protecting against taxpayer costs. Second, the employee survey does not directly support some of the conclusions that the GAO draws from those responses, and only 24% of the respondents were in the Export Finance area which handles the underwriting of EXIM transactions. Third, EXIM has been very effective in preventing, detecting, and prosecuting fraud in EXIM transactions. Fourth, the Report and Employee Survey does not clearly and consistently distinguish between fraud and fraud risk, which may lead to confusion in both the survey responses and the analysis in the Report. The anti-fraud program and practices at EXIM are subject to continuous improvement, and EXIM endeavors to create a culture of fraud risk awareness throughout the agency.

We appreciate your acknowledgement of the very broad support for EXIM's anti-fraud program within the Bank community. This support is a major factor in the effectiveness of the Bank's anti-fraud program, resulting in both the Bank's low default rate of 0.438% as of March 2018 and the Bank's low rate of proven fraud of barely 0.07% for short-term and medium-term transactions over the past 10 years. We note that there are no known fraud occurrences in the long-term program. GAO's employee survey on this matter also provided very gratifying evidence of the effectiveness of the Bank's anti-fraud training efforts over the past 10 plus years. The employee survey responses indicated very high levels of awareness of fraud risks among Bank

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov



Reducing Risk. Unleashing Opportunity.

employees and very low – single-digit – disagreement with the Bank's approach to preventing, detecting, and prosecuting fraud in Bank transactions. This very high level of employee awareness of fraud risks and strong support for the Bank's anti-fraud efforts contributes to the team approach and no doubt helps explain the very low levels of proven fraud against the Bank.

Inasmuch as measuring the rate of actual fraud is necessarily imprecise, the Bank has taken a multi-layered approach to assessing the incidence of fraud in Bank transactions. The Bank's low default rate is a strong indicator of the low rate of fraud in that, over time, all transactional fraud results in a default. The Bank's default rate averaged 0.44% over the past 10 years, and the continuous improvement in Bank practices has assisted with an overall decline in the default rate from 1.1% in 2008 to the current rate of 0.438%. In addition, EXIM transactions in which fraud has been admitted or proven in court over the past 10 years represents a proven fraud rate of barely 0.07% of overall short and medium term transactions. Again, this is a conservative figure because it does not include \$123.8 billion of authorizations in the Bank's long-term transactions over the same period for which there were no known fraud occurrences.

The foregoing data, and other indicators, shows the anti-fraud controls the Bank has put into place have produced a low rate of proven fraud over a long period of time, and they reveal a declining incidence of fraud. As you know, the Bank, for many years, has had procedures for the prevention, detection, and prosecution of fraud, and those procedures were written into a formal Bank policy in 2015. Pursuant to those procedures, the Bank's Office of General Counsel refers all matters in which there is even the merest suspicion of fraud or other illegal activity to the Bank's Office of Inspector General. At the same time, the Bank's Office of Inspector General alerts the Bank regarding any intelligence it receives (that it is legally permitted to share) of potential fraud threats to the Bank. These referrals in both directions have declined significantly over the past several years. The Bank interprets this as a testament to the effectiveness of the Bank's anti-fraud procedures, a key part of which is aggressive investigation and prosecution by the Bank's Office of Inspector General. In addition to the numbers of referrals, the Bank monitors the nature of suspected fraud in the referrals made between the Bank and the Office of Inspector General. For example, over the past several years, the referrals to the Office of Inspector General have shifted from referrals based on relatively strong evidence to referrals based on the merest suspicion of fraud. The Bank has recently formalized the process for tracking the referrals to the Office of Inspector General, as well as the results of such referrals.

We also appreciate the GAO's acknowledgement of the Bank's early commencement of an Enterprise Risk Management system. As you note, in July 2016, OMB Circular A-123 encouraged Government Corporations such as EXIM to use the

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov



Reducing Risk. Unleashing Opportunity.

GAO's "A Framework for Managing Fraud Risks in Federal Programs" (the "GAO Fraud Framework") as guidance for anti-fraud programs. Before that, in 2013, the Bank had already embarked on establishing an Enterprise Risk Framework pursuant to the leading principles laid out in Committee of Sponsoring Organizations of the Treadway Commission (COSO). Three months after the July 2016 update to OMB Circular A-123, GAO commenced this audit. During this audit, the GAO has encouraged the Bank to formalize some aspects of its anti-fraud program in line with the GAO Fraud Framework. The Bank commenced its implementation and those efforts continue to move forward.

Additionally, the Bank appreciates the GAO's acknowledgement of the Bank's continuous improvement in its anti-fraud efforts. The GAO's suggestion that "the Bank Needs to Continue to Improve Fraud Risk Management" is taken as a truism here at the Bank and is an integral part of the Bank's anti-fraud program. The Bank's anti-fraud program is dynamic and has evolved over time and will continue to evolve as the Bank learns more and more about the most effective ways to prevent, detect, and prosecute fraud. The Bank's first line of defense against fraud in Bank transactions is the Bank's underwriting process. From fiscal year 2014 to date, the Bank has processed 14,905 medium term and short term transactions and has approved 12,931 of those, with a default rate consistently lower than 0.5% for these years. These numbers strongly suggest that the Bank's underwriters have displayed good credit and fraud recognition in filtering out those transactions that did not provide appropriate assurance of repayment or were otherwise harmful to the Bank. The Bank does not review rejected transactions for fraud because no taxpayer money is at risk; however, anything suspicious is referred to Office of the General Counsel and the Office of Inspector General. The Bank has also authorized 112 long-term transactions during the same period of time, none of which have proven to contain fraud.

Further, to contextualize EXIM's fraud risk management practices and vulnerabilities, some baseline metrics for government or financial services overall are useful. Across sectors, measuring the amount and rate of fraud is difficult. There is a lack of concrete data and metrics surrounding the prevalence and degree of fraud. Thus, it is difficult for EXIM to compare the effectiveness of its fraud risk practices along quantifiable measures. However, EXIM has already implemented a variety of fraud risk management practices to which EXIM's low rate of fraud can be attributed. The current set of fraud risk management internal controls is expansive, covering both pre- and post-approval transaction processes. While EXIM's goal of continuous improvement in the fraud risk management space aligns with GAO's report, there is little effort devoted in the report to outlining the efficacy of the current practices. See Annex A for further information about overall industry fraud metrics, as well as a non-exhaustive list of current fraud internal controls.

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

**Appendix III: Comments from the Export-
Import Bank of the United States**



Reducing Risk. Unleashing Opportunity.

GAO has made seven recommendations in this report regarding the Bank's fraud risk assessment activities. These recommendations deal primarily with tailoring activities to the four components of the GAO Fraud Risk Framework, and the Bank's responses to the recommendations are attached.

Sincerely,

Ambassador Jeffrey D. Gerrish
President and Chairman (Acting) of the Export-
Import Bank of the United States
Deputy United States Trade Representative for
Asia, Europe, the Middle East, and Industrial
Competitiveness

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov



Reducing Risk. Unleashing Opportunity.

GAO Recommendations and EXIM Management Response:

Recommendation 1: The acting Bank president and Board chairman should ensure that the Bank evaluates and implements methods to further promote and sustain an antifraud tone that permeates the Bank's organizational culture, as described in GAO's Fraud Risk Framework. This should include consideration of requiring training on fraud risks relevant to Bank programs, for new employees and all employees on an ongoing basis, with the training to include identifying roles and responsibilities in fraud risk management activities across the Bank.

Management Response: The Bank agrees with this recommendation.

The Bank will continue to evaluate and implement methods to promote and sustain an antifraud tone that permeates the Bank's organizational culture. This will include allocating resources and providing regular training to staff involved in export credit activities across the Bank. The Bank will consider requiring training for all employees.

Recommendation 2: As the agency begins efforts to plan and conduct regular, comprehensive fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that the Bank's risk assessments and profile address not only known methods of fraud, including those that are absent from its current risk register, but other inherent fraud risks as well.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will include known and inherent risks in its risk assessments and profile, including consideration of other inherent risks that have not been experienced by the Bank.

Recommendation 3: As the agency begins efforts to plan and conduct regular, comprehensive fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that that risk profile includes risk tolerances that are specific and measurable.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will seek to ensure that its fraud risk profile tolerances are specific and measurable through available information related to other government agencies, financial institutions, and historical identifiable results at the Bank.

Recommendation 4: The acting Bank president and Board chairman should ensure that the Bank develops and implements an antifraud strategy with specific control

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

Appendix III: Comments from the Export-Import Bank of the United States



Reducing Risk. Unleashing Opportunity.

activities, based upon the results of comprehensive fraud risk assessments and a corresponding fraud risk profile, as provided in GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework and subject to a benefit-cost analysis, the Bank will look to correlate its existing control activities with fraud risk assessments and a fraud risk profile and will develop and implement additional control activities that are also determined by a fraud risk assessment and corresponding profile.

Recommendation 5: The acting Bank president and Board chairman should ensure that the Bank identifies, and then implements, the best options for sharing more fraud-related information – including details of fraud case referrals and outcomes – among Bank staff, to help build fraud awareness, as described in GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

The Bank will share adjudicated information that results in evidence of fraudulent or other illegal activity with staff working in export credit activities. The Bank cannot more broadly share, within the Bank, the details of fraud case referrals. However, the Bank is exploring technological ways that the Bank's referral information can be automatically checked against active transaction participants so as to protect the Bank without actually broadly sharing the details of the referrals. Additionally, the Bank is strengthening its procedures with the Office of Inspector General to obtain timely updates of referred matters that have been closed out by the Office of Inspector General. As mentioned before, referrals to the Office of Inspector General can be based on speculative evidence and, if shared before fraud or other illegal activity is proven, could cause tremendous harm to the referred party. Additionally, broad sharing of referral details significantly raises the risk of a leak of information outside of the Bank or even to the referred party. This could significantly undermine any criminal investigation the Office of Inspector General may wish to undertake.

Recommendation 6: The acting Bank president and Board chairman should lead efforts to collaborate with the Bank's Office of Inspector General to identify feasible, cost-effective means to systematically track outcomes of fraud referrals from the Bank to the Office of Inspector General, including creating a means to link the Office of Inspector General's proven cases of fraud to the specific Bank transactions from which the Office of Inspector General actions arise. If any such means are found to be feasible and cost-effective, the acting Bank president and Board chairman should direct appropriate staff to implement them, with such information to be used for purposes consistent with GAO's Fraud Risk Framework, such as data analytics.

Management Response: The Bank agrees with this recommendation.

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

Appendix III: Comments from the Export-Import Bank of the United States



Reducing Risk. Unleashing Opportunity.

Consistent with GAO's Fraud Risk Framework, the Bank is currently working with the Office of Inspector General to identify a cost-effective mechanism to systematically track outcomes of fraud referrals from the Bank to the Office of Inspector General. To the extent that proven cases of fraud are specifically linked to identifiable transactions, that information will also be included in the tracking system.

Recommendation 7: The acting Bank president and Board chairman should ensure that the Bank monitors and evaluates outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and that it subsequently adapts antifraud activities or implements new ones, as determined to be appropriate and consistent with GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will monitor and evaluate outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and adapt existing controls or implement new controls, subject to a benefit-cost analysis.

We thank the GAO for its efforts to ensure the Bank's policies and procedures continue to improve and to protect the U.S. taxpayer from fraud, waste, and abuse.

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov



Reducing Risk. Unleashing Opportunity.

Annex A: Industry Fraud Metrics and Current EXIM Internal Controls

Across sectors, measuring the amount and rate of fraud is difficult. Not all fraud is detected, and not all fraud detected is reported. As a result, there is a significant lack of concrete data and metrics surrounding the prevalence and degree of fraud. Thus, it is difficult for EXIM to compare its own fraud risk practices' effectiveness along quantifiable measures. However, some aggregate baseline metrics exist via large-scale surveys conducted by organizations such as Ernst & Young (EY) and PricewaterhouseCoopers (PWC).

Fraud Perpetrators: PWC's 2018 Global Economic Crime and Fraud Survey finds that 52% of fraud cases were done by internal actors, while 41% were done by external actors, with 68% of external fraud actors being 'frenemies' of the institution, such as agents, customers, vendors, etc. Conversely, for the financial services sector specifically, Ernst and Young's 2016 Global Economic Crime Survey finds that 29% of fraud cases were committed by internal perpetrators and 59% were committed by external perpetrators. At EXIM, the internal controls in place cover both internal and external fraud cases.

EXIM Internal Controls: For external fraud, which is a major focus in EXIM's fraud risk management practice, the agency has a robust set of existing anti-fraud controls. On the pre-authorization stage of transaction application and underwriting, controls include an underwriting process guided by the Loan, Insurance, and Guarantee Manual, Credit Review & Compliance checks, certification requirements, Character, Reputational, and Transaction Integrity and Know-Your-Customer practices, and credit administration invoice review processes. For internal fraud, the system of delegated authority, Credit Review and Compliance checks, manager oversight, and the clear underwriting process all provide effective monitoring and controls. Existing anti-fraud internal controls include but are not limited to the practices outline on the following table:

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

Appendix III: Comments from the Export-Import Bank of the United States



Reducing Risk. Unleashing Opportunity.

| Pre-Approval: Transaction Application and Underwriting | | |
|--|----------------------------|---|
| Underlying Fraud Factor per EXIM's Draft Fraud Risk Toolkit | GAO-Highlighted Evaluation | EXIM Existing Internal Controls |
| A) Business Volume Goals; B) Complexity of Process; C) Reliance on Application Documents; D) Reliance on Certifications; E) Level of Manual Intervention; F) Technological Systems and Critical Data | Underwriting | 1) Robust and detailed underwriting process and trainings; 2) Credit Review and Compliance (CRC) Controls and Reviews; 3) Certification Requirements; 4) Independent Engineering and Environment (E&E) Acquisition List Review Process; 5) Credit Administration Invoice Review Process; 6) Coordination between Acquisition List and Credit Administration; 7) Character, Reputational, and Transaction Integrity (CRTI) Controls; 8) Know-Your-Customer (KYC) Practices; 9) Sign Off Process and Internal Checks; 10) Relationship with Exporters, Lenders, and Borrowers; 11) Frequent Site Visits / Due Diligence; 12) EXIM Continual Review of Documentation; 13) Separate Underwriting and Asset Management Teams; 14) Training; |
| A) Complexity of Process; B) Reliance on Application Documents; C) Level of Manual Intervention; D) Technological Systems and Critical Data | Database Checks | |
| A) Complexity of Process; B) Reliance on Application Documents; C) Reliance on Operational (Disbursement) Documents; D) Certifications; E) Vague or No Description of Goods | Enhanced Due Diligence | |
| A) Reliance on Application Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; | 'Red Flag' Indicators | |

| Post-Approval: Asset Management and Monitoring | | |
|---|----------------------------|---|
| Underlying Fraud Factor per EXIM's Draft Fraud Framework | GAO-Highlighted Evaluation | EXIM Existing Internal Controls |
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; | Default | 1) Credit Review and Compliance (CRC) Controls and Reviews; 2) Independent Engineering and Environment (E&E) Acquisition List Review Process; 3) Certification Requirements; 4) Training; 5) EXIM Review of Documents pre-Disbursement; 6) Lender and Agent Review Prior to Submission; 7) MARAD Review; 8) Relationship with Clients; 9) Separate Underwriting and Asset Management Teams; |
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; D) Technological Systems and Critical Data | Compliance Reviews | |
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; D) Technological Systems and Critical Data | On-going Monitoring | |

811 Vermont Avenue, NW Washington, DC 20571 | Main: 202 565 3946 | Fax: 202 565 3380

exim.gov

Appendix IV: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan, (202) 512-6722 or bagdoyans@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jonathon Oldmixon (Assistant Director), Marcus Corbin, Carrie Davidson, David Dornisch, Paulissa Earl, Colin Fallon, Dennis Fauber, Kimberly Gianopoulos, Gina Hoover, Farahnaaz Khakoo-Mausel, Heather Latta, Flavio Martinez, Maria McMullen, Carl Ramirez, Christopher H. Schmitt, Sabrina Streagle, and Celia Thomas made key contributions to this report.

Appendix V: Accessible Data

Data Table

Accessible Data for Figure 2: Export-Import Bank of the United States Exposure by Product Type, Geographic Region, and Economic Sector, Fiscal Year 2017

| n/a | n/a | Billions of Dollars |
|--------------------------|---------------------------------|---------------------|
| Product | Loan guarantees | \$46.6 |
| | Direct loans | \$21.3 |
| | Credit insurance | \$3.6 |
| | Other | \$1.0 |
| Geographic region | Asia | \$18.1 |
| | Latin America and the Caribbean | \$13.4 |
| | Europe | \$11.8 |
| | Middle East and North Africa | \$11.2 |
| | Oceania | \$6.7 |
| | North America | \$4.4 |
| | Sub-Saharan Africa | \$4.4 |
| | Other | \$2.4 |
| Economic sector | Aircraft | \$35.2 |
| | Manufacturing | \$12.6 |
| | Oil & Gas | \$11.3 |
| | Power Projects | \$4.2 |
| | All Other | \$9.1 |

Agency Comment Letter

Accessible Text for Appendix III Comments from the Export-Import Bank of the United States

Page 1

June 29, 2018

Seto J. Bagdoyan,
Director, Forensic Audits and Investigative Service
U.S. Government Accountability Office
441 G St. NW
Washington, D.C. 20584

Dear Mr. Bagdoyan:

Thank you for providing the Export-Import Bank of the United States ("EXIM" or the "Bank") with the Government Accountability Office (GAO) draft report, "The Bank Needs to Continue to Improve Fraud Risk Management" (July 2018). The Bank supports the GAO's work and audits which complement the Bank's efforts to continuously improve its practices and procedures. EXIM Bank is proud of its cooperative relationship with GAO.

As highlighted in the General Comments A - D in the Omissions and Errata List response from EXIM to the GAO, there are several chief concerns EXIM would like to raise with the Report findings. First and foremost, EXIM keeps substantial reserves for losses protecting against taxpayer costs. Second, the employee survey does not directly support some of the conclusions that the GAO draws from those responses, and only 24% of the respondents were in the Export Finance area which handles the underwriting of EXIM transactions. Third, EXIM has been very effective in preventing, detecting, and prosecuting fraud in EXIM transactions. Fourth, the Report and Employee Survey does not clearly and consistently distinguish between fraud and fraud risk, which may lead to confusion in both the survey responses and the analysis in the Report. The anti-fraud program and practices at EXIM are subject to continuous improvement, and EXIM endeavors to create a culture of fraud risk awareness throughout the agency.

We appreciate your acknowledgement of the very broad support for EXIM's anti-fraud program within the Bank community. This support is a major factor in the effectiveness of the Bank's anti-fraud program, resulting in both the Bank's low default rate of 0.438% as of March 2018 and the Bank's low rate of proven fraud of barely 0.07% for short-term and medium-term transactions over the past 10 years. We note that there are no known fraud occurrences in the long-term program. GAO's employee survey on this matter also provided very gratifying evidence of the effectiveness of the Bank's anti-fraud training efforts over the past 10 plus years. The employee survey responses indicated very high levels of awareness of fraud risks among Bank

Page 2

employees and very low - single-digit - disagreement with the Bank's approach to preventing, detecting, and prosecuting fraud in Bank transactions. This very high level of employee awareness of fraud risks and strong

support for the Bank's anti-fraud efforts contributes to the team approach and no doubt helps explain the very low levels of proven fraud against the Bank.

Inasmuch as measuring the rate of actual fraud is necessarily imprecise, the Bank has taken a multi-layered approach to assessing the incidence of fraud in Bank transactions. The Bank's low default rate is a strong indicator of the low rate of fraud in that, over time, all transactional fraud results in a default. The Bank's default rate averaged 0.44% over the past 10 years, and the continuous improvement in Bank practices has assisted with an overall decline in the default rate from 1.1% in 2008 to the current rate of 0.438%. In addition, EXIM transactions in which fraud has been admitted or proven in court over the past 10 years represents a proven fraud rate of barely 0.07% of overall short and medium term transactions. Again, this is a conservative figure because it does not include \$123.8 billion of authorizations in the Bank's long-term transactions over the same period for which there were no known fraud occurrences.

The foregoing data, and other indicators, shows the anti-fraud controls the Bank has put into place have produced a low rate of proven fraud over a long period of time, and they reveal a declining incidence of fraud. As you know, the Bank, for many years, has had procedures for the prevention, detection, and prosecution of fraud, and those procedures were written into a formal Bank policy in 2015. Pursuant to those procedures, the Bank's Office of General Counsel refers all matters in which there is even the merest suspicion of fraud or other illegal activity to the Bank's Office of Inspector General. At the same time, the Bank's Office of Inspector General alerts the Bank regarding any intelligence it receives (that it is legally permitted to share) of potential fraud threats to the Bank. These referrals in both directions have declined significantly over the past several years. The Bank interprets this as a testament to the effectiveness of the Bank's anti-fraud procedures, a key part of which is aggressive investigation and prosecution by the Bank's Office of Inspector General. In addition to the numbers of referrals, the Bank monitors the nature of suspected fraud in the referrals made between the Bank and the Office of Inspector General. For example, over the past several years, the referrals to the Office of Inspector General have shifted from referrals based on relatively strong evidence to referrals based on the merest suspicion of fraud. The Bank has recently formalized the process for tracking the referrals to the Office of Inspector General, as well as the results of such referrals.

We also appreciate the GAO's acknowledgement of the Bank's early commencement of an Enterprise Risk Management system. As you note, in July 2016, OMB Circular A-123 encouraged Government Corporations such as EXIM to use the

Page 3

GAO's "A Framework for Managing Fraud Risks in Federal Programs" (the "GAO Fraud Framework") as guidance for anti-fraud programs. Before that, in 2013, the Bank had already embarked on establishing an Enterprise Risk Framework pursuant to the leading principles laid out in Committee of Sponsoring Organizations of the Treadway Commission (COSO). Three months after the July 2016 update to OMB Circular A-123, GAO commenced this audit. During this audit, the GAO has encouraged the Bank to formalize some aspects of its anti-fraud program in line with the GAO Fraud Framework. The Bank commenced its implementation and those efforts continue to move forward.

Additionally, the Bank appreciates the GAO's acknowledgement of the Bank's continuous improvement in its anti-fraud efforts. The GAO's suggestion that "the Bank Needs to Continue to Improve Fraud Risk Management" is taken as a truism here at the Bank and is an integral part of the Bank's anti-fraud program. The Bank's anti-fraud program is dynamic and has evolved over time and will continue to evolve as the Bank learns more and more about the most effective ways to prevent, detect, and prosecute fraud. The Bank's first line of defense against fraud in Bank transactions is the Bank's underwriting process. From fiscal year 2014 to date, the Bank has processed 14,905 medium term and short term transactions and has approved 12,931 of those, with a default rate consistently lower than 0.5% for these years. These numbers strongly suggest that the Bank's underwriters have displayed good credit and fraud recognition in filtering out those transactions that did not provide appropriate assurance of repayment or were otherwise harmful to the Bank. The Bank does not review rejected transactions for fraud because no taxpayer money is at risk; however, anything suspicious is referred to Office of the General Counsel and the Office of Inspector General. The Bank has also authorized 112 long-term transactions during the same period of time, none of which have proven to contain fraud.

Further, to contextualize EXIM's fraud risk management practices and vulnerabilities, some baseline metrics for government or financial services overall are useful. Across sectors, measuring the amount and rate of fraud is difficult. There is a lack of concrete data and metrics surrounding the prevalence and degree of fraud. Thus, it is difficult for EXIM to compare the effectiveness of its fraud risk practices along quantifiable measures. However, EXIM has already implemented a variety of fraud risk management practices to which EXIM's low rate of fraud can be attributed. The current set of fraud risk management internal controls is expansive, covering both pre- and post-approval transaction processes. While EXIM's goal of continuous improvement in the fraud risk management space aligns with GAO's report, there is little effort devoted in the report to outlining the efficacy of the current practices. See Annex A for further information about overall industry fraud metrics, as well as a non-exhaustive list of current fraud internal controls.

Page 4

GAO has made seven recommendations in this report regarding the Bank's fraud risk assessment activities. These recommendations deal primarily with tailoring activities to the four components of the GAO Fraud Risk Framework, and the Bank's responses to the recommendations are attached.

Sincerely,

Ambassador Jeffrey D. Gerrish

President and Chairman (Acting) of the Export-Import Bank of the United States

Deputy United States Trade Representative for Asia, Europe, the Middle East, and Industrial Competitiveness

Page 5

GAO Recommendations and EXIM Management Response:

Recommendation 1: The acting Bank president and Board chairman should ensure that the Bank evaluates and implements methods to further promote and sustain an antifraud tone that permeates the Bank's organizational culture, as described in GAO's Fraud Risk Framework. This should include consideration of requiring training on fraud risks relevant to Bank programs, for new employees and all employees on an ongoing basis, with the training to include identifying roles and responsibilities in fraud risk management activities across the Bank.

Management Response: The Bank agrees with this recommendation.

The Bank will continue to evaluate and implement methods to promote and sustain an antifraud tone that permeates the Bank's organizational culture. This will include allocating resources and providing regular training to staff involved in export credit activities across the Bank. The Bank will consider requiring training for all employees.

Recommendation 2: As the agency begins efforts to plan and conduct regular, comprehensive fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that the Bank's risk assessments and profile address not only known methods of fraud, including those that are absent from its current risk register, but other inherent fraud risks as well.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will include known and inherent risks in its risk assessments and profile, including consideration of other inherent risks that have not been experienced by the Bank.

Recommendation 3: As the agency begins efforts to plan and conduct regular, comprehensive fraud risk assessments and to determine a fraud risk profile, the acting Bank president and Board chairman should ensure that that risk profile includes risk tolerances that are specific and measurable.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will seek to ensure that its fraud risk profile tolerances are specific and measurable through available information related to other government agencies, financial institutions, and historical identifiable results at the Bank.

Recommendation 4: The acting Bank president and Board chairman should ensure that the Bank develops and implements an antifraud strategy with specific control

Page 6

activities, based upon the results of comprehensive fraud risk assessments and a corresponding fraud risk profile, as provided in GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework and subject to a benefit-cost analysis, the Bank will look to correlate its existing control activities with fraud risk assessments and a fraud risk profile and will develop and implement additional control activities that are also determined by a fraud risk assessment and corresponding profile.

Recommendation 5: The acting Bank president and Board chairman should ensure that the Bank identifies, and then implements, the best options for sharing more fraud-related information - including details of fraud case referrals and outcomes- among Bank staff, to help build fraud awareness, as described in GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

The Bank will share adjudicated information that results in evidence of fraudulent or other illegal activity with staff working in export credit activities. The Bank cannot more broadly share, within the Bank, the details of fraud case referrals. However, the Bank is exploring technological ways that the Bank's referral information can be automatically checked against active transaction participants so as to protect the Bank without actually broadly sharing the details of the referrals. Additionally, the Bank is strengthening its procedures with the Office of Inspector General to obtain timely updates of referred matters that have been closed out by the Office of Inspector General. As mentioned before, referrals to the Office of Inspector General can be based on speculative evidence and, if shared before fraud or other illegal activity is proven, could cause tremendous harm to the referred party. Additionally, broad sharing of referral details significantly raises the risk of a leak of information outside of the Bank or even to the referred party. This could significantly undermine any criminal investigation the Office of Inspector General may wish to undertake.

Recommendation 6: The acting Bank president and Board chairman should lead efforts to collaborate with the Bank's Office of Inspector General to identify feasible, cost-effective means to systematically track outcomes of fraud referrals from the Bank to the Office of Inspector General, including creating a means to link the Office of Inspector General's proven cases of fraud to the specific Bank transactions from which the Office of Inspector General actions arise. If any such means are found to be feasible and cost-effective, the acting Bank president and Board chairman should direct appropriate staff to implement them, with such information to be used for purposes consistent with GAO's Fraud Risk Framework, such as data analytics.

Management Response: The Bank agrees with this recommendation.

Page 7

Consistent with GAO's Fraud Risk Framework, the Bank is currently working with the Office of Inspector General to identify a cost-effective mechanism to systematically track outcomes of fraud referrals from the Bank to the Office of Inspector General. To the extent that proven cases of fraud are specifically linked to identifiable transactions, that information will also be included in the tracking system.

Recommendation 7: The acting Bank president and Board chairman should ensure that the Bank monitors and evaluates outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and that it subsequently adapts antifraud activities or implements new ones, as determined to be appropriate and consistent with GAO's Fraud Risk Framework.

Management Response: The Bank agrees with this recommendation.

Consistent with GAO's Fraud Risk Framework, the Bank will monitor and evaluate outcomes of fraud risk management activities, using a risk-based approach and outcome-oriented metrics, and adapt existing controls or implement new controls, subject to a benefit-cost analysis.

We thank the GAO for its efforts to ensure the Bank's policies and procedures continue to improve and to protect the U.S. taxpayer from fraud, waste, and abuse.

Page 8

Annex A: Industry Fraud Metrics and Current EXIM Internal Controls

Across sectors, measuring the amount and rate of fraud is difficult. Not all fraud is detected, and not all fraud detected is reported. As a result, there is a significant lack of concrete data and metrics surrounding the prevalence and degree of fraud. Thus, it is difficult for EXIM to compare its own fraud risk practices' effectiveness along quantifiable measures. However, some aggregate baseline metrics exist via large-scale surveys conducted by organizations such as Ernst & Young (EY) and PricewaterhouseCoopers (PWC).

Fraud Perpetrators: PWC's 2018 Global Economic Crime and Fraud Survey finds that 52% of fraud cases were done by internal actors, while 41% were done by external actors, with 68% of external fraud actors being 'frenemies' of the institution, such as agents, customers, vendors, etc. Conversely, for the financial services sector specifically, Ernst and Young's 2016 Global Economic Crime Survey finds that 29% of fraud cases were committed by internal perpetrators and 59% were committed by external perpetrators. At EXIM, the internal controls in place cover both internal and external fraud cases.

EXIM Internal Controls: For external fraud, which is a major focus in EXIM's fraud risk management practice, the agency has a robust set of existing anti-fraud controls. On the pre-authorization stage of transaction application and underwriting, controls include an underwriting process guided by the Loan, Insurance, and Guarantee Manual, Credit Review & Compliance checks, certification requirements, Character, Reputational, and Transaction Integrity and Know-Your-Customer practices, and credit administration invoice review processes. For internal fraud, the system of delegated authority, Credit Review and Compliance checks, manager oversight, and the clear underwriting process all provide effective monitoring and controls. Existing anti-fraud internal controls include but are not limited to the practices outline on the following table:

Pre-Approval: Transaction Application and Underwriting

| Underlying Fraud Factor per EXIM's Draft Fraud Risk Toolkit | GAO-Highlighted Evaluation | EXIM Existing Internal Controls |
|--|-----------------------------------|---|
| A) Business Volume Goals; B) Complexity of Process; C) Reliance on Application Documents; D) Reliance on Certifications; E) Level of Manual Intervention; F) Technological Systems and Critical Data | Underwriting | <ol style="list-style-type: none"> 1. Robust and detailed underwriting process and trainings; 2. Credit Review and Compliance (CRC) Controls and Reviews 3. Certification Requirements; 4. Independent Engineering and Environment (E&E) Acquisition List Review Process; 5. Credit Administration Invoice Review Process; 6. Coordination between Acquisition List and Credit Administration; 7. Character, Reputational, and Transaction Integrity (CRTI) Controls; 8. Know-Your-Customer (KYC) Practices; 9. Sign Off Process and Internal Checks; 10. Relationship with Exporters, Lenders, and Borrowers; 11. Frequent Site Visits/ Due Diligence; 12. EXIM Continual Review of Documentation; 13. Separate Underwriting and Asset Management Teams; 14. Training; |
| A) Complexity of Process; B) Reliance on Application Documents; C) Level of Manual Intervention; D) Technological Systems and Critical Data | Database Checks | |
| A) Complexity of Process; B) Reliance on Application Documents; C) Reliance on Operational (Disbursement) Documents; D) Certifications; E) Vague or No Description of Goods | Enhanced Due Diligence | |
| A) Reliance on Application Documents; B) Reliance on Certifications; C) Vague or No Description of Goods | 'Red Flag Indicators | |

Post-Approval: Asset Management and Monitoring

| Underlying Fraud Factor per EXIM's Draft Fraud Framework | GAO-Highlighted Evaluation | EXIM Existing Internal Controls |
|---|----------------------------|---|
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; | Default | <ol style="list-style-type: none"> 1. Credit Review and Compliance (CRC) Controls and Reviews. 2. Independent Engineering and Environment (E&E) Acquisition List Review Process; |
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; D) Technological Systems and Critical Data | Compliance Reviews | <ol style="list-style-type: none"> 3. Certification Requirements; 4. Training; 5. EXIM Review of Documents pre-Disbursement; |
| A) Reliance on Operational (Disbursement) Documents; B) Reliance on Certifications; C) Vague or No Description of Goods; D) Technological Systems and Critical Data | On-going Monitoring | <ol style="list-style-type: none"> 6. Lender and Agent Review Prior to Submission 7. MARAD Review; 8. Relationship with Clients; 9. Separate Underwriting and Asset Management Teams; |

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's website (<https://www.gao.gov>). Each weekday afternoon, GAO posts on its website newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to <https://www.gao.gov> and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's website, <https://www.gao.gov/ordering.htm>.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

Connect with GAO

Connect with GAO on [Facebook](#), [Flickr](#), [Twitter](#), and [YouTube](#).
Subscribe to our [RSS Feeds](#) or [E-mail Updates](#). Listen to our [Podcasts](#).
Visit GAO on the web at <https://www.gao.gov>.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Website: <https://www.gao.gov/fraudnet/fraudnet.htm>

Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Orice Williams Brown, Managing Director, WilliamsO@gao.gov, (202) 512-4400,
U.S. Government Accountability Office, 441 G Street NW, Room 7125,
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Strategic Planning and External Liaison

James-Christian Blockwood, Managing Director, spel@gao.gov, (202) 512-4707
U.S. Government Accountability Office, 441 G Street NW, Room 7814,
Washington, DC 20548