



September 2022

EXPORT-IMPORT BANK

Additional
Documentation about
Stakeholder Roles
and Clarity about
Fraud Risks Would
Strengthen Antifraud
Efforts

GAO Highlights

Highlights of [GAO-22-105340](#), a report to congressional committees

Why GAO Did This Study

EXIM's mission is to support American jobs by facilitating the export of U.S. goods and services. Taxpayers could be responsible for losses arising from EXIM's operations, including losses due to fraud. The 2019 legislation reauthorizing EXIM included an antifraud requirement. Specifically, the legislation stated that EXIM shall deny an application for assistance if an individual has been convicted of an act of fraud or corruption in connection with an application for support from EXIM in the prior 5 years.

Since 2015, GAO has been mandated by law to periodically review EXIM's antifraud controls. This report assesses the extent to which EXIM has (1) designed and implemented an antifraud strategy and collaborated with stakeholders to ensure its implementation; and (2) established responsibilities and designed and implemented control activities to address its antifraud requirement as required by legislation. GAO assessed EXIM's activities against leading practices, reviewed EXIM documentation, and interviewed EXIM managers. GAO also reviewed EXIM transactions from January 1, 2020, to December 31, 2021—the most recent data available when GAO began its work.

What GAO Recommends

GAO is making two recommendations to EXIM to (1) demonstrate links to its highest residual fraud risks within its antifraud strategy, and (2) document the roles and responsibilities of the external partners responsible for fraud controls. EXIM agreed with GAO's recommendations.

View [GAO-22-105340](#). For more information, contact Seto J. Bagdoyan, (202) 512-4749, bagdoyans@gao.gov

September 2022

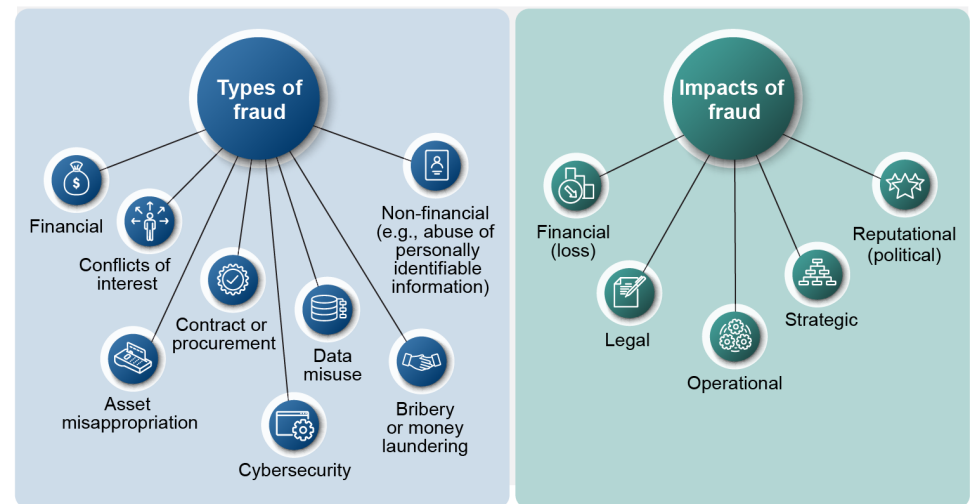
EXPORT-IMPORT BANK

Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts

What GAO Found

The Export-Import Bank of the United States (EXIM) has designed and implemented an antifraud strategy and collaborated with stakeholders to ensure its implementation, but the strategy is missing key elements. EXIM's strategy includes specific control activities to prevent and detect fraud in accordance with leading practices, which reflect the types and impacts of fraud (see figure).

Types and Impacts of Potential Fraud at Export-Import Bank of the United States



Source: GAO analysis of Export-Import Bank of the United States information and [stas111/stock.adobe.com](#) (images). | GAO-22-105340

Further, EXIM identified risks that remained even after being mitigated by existing control activities that exceed its risk appetite. For those residual risks, EXIM identified and documented how the agency will respond to them, which better positions EXIM to prevent fraud risks that exceed its appetite. However, EXIM did not link these residual risks to its antifraud strategy. As described in fraud risk management leading practices, doing so helps program managers focus their activities. Without these linkages, EXIM cannot be assured that it is adequately addressing risks in a dynamic risk environment or that its approach addresses the fraud risks it identified and prioritized. EXIM also works with outside stakeholders, such as lenders and export credit insurance partners, to process transactions that carry EXIM's guarantees. However, EXIM did not document these external stakeholders' roles and responsibilities for fraud controls in the strategy to ensure that all parties, including outside lenders and export credit insurance partners, understand their fraud-related responsibilities.

EXIM has established responsibilities and designed and implemented control activities to address its antifraud requirement, as required by its reauthorizing legislation. GAO also reviewed EXIM 2020-2021 transaction data to determine if EXIM had appropriately denied applications by parties convicted of EXIM-related fraud or corruption charges. GAO's analysis did not identify any relevant convicted parties within the EXIM transaction data.

Contents

Letter		1
	Background	4
	EXIM Has Designed and Implemented an Overall Antifraud Strategy and Collaborated with Stakeholders to Ensure Its Implementation, but the Strategy Is Missing Key Elements	12
	EXIM Has Established Responsibilities and Designed and Implemented Control Activities to Address Its Statutory Antifraud Requirement	24
	Conclusions	30
	Recommendations for Executive Action	31
	Agency Comments	31
Appendix I	Objectives, Scope, and Methodology	34
Appendix II	Comments from the Export-Import Bank of the United States	38
Appendix III	GAO Contact and Staff Acknowledgments	40
Figures		
	Figure 1: Export-Import Bank of the United States' (EXIM) Financing Programs and Program Terms	5
	Figure 2: Export-Import Bank of the United States' (EXIM) Authorizations by Term and Program for Fiscal Years 2020 and 2021	6
	Figure 3: The Four Components of the Fraud Risk Framework and Selected Leading Practices	8
	Figure 4: Roles and Responsibilities for Fraud Risk Management at Export-Import Bank of the United States	14
	Figure 5: Types and Impacts of Potential Fraud at Export-Import Bank of the United States (EXIM)	15
	Figure 6: Export-Import Bank of the United States' (EXIM) External Stakeholders' Roles and Responsibilities for Antifraud Controls within the Antifraud Strategy	22
	Figure 7: Export-Import Bank of the United States' (EXIM) Character, Reputational, and Transaction Integrity (CRTI) Process Using the Convicted Parties List	26

Figure 8: Monitoring of Export-Import Bank of the United States'
(EXIM) Financing Programs Section 406 Compliance

29

Abbreviations

CPL	Convicted Parties List
CRTI	character, reputational, and transaction integrity
DAL	delegated authority lending
ECI	Export Credit Insurance
EXIM	Export-Import Bank of the United States
FRO	Fraud Risk Oversight team
KYC	Know Your Customer
OGC	Office of the General Counsel
OIG	Office of Inspector General
OMB	Office of Management and Budget

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.



September 27, 2022

Congressional Committees

The mission of the Export-Import Bank of the United States (EXIM) is to support American jobs by facilitating the export of U.S. goods and services.¹ To support these exports, EXIM offers multiple forms of assistance: direct loans, loan guarantees, working capital loan guarantees, and export credit insurance. EXIM is backed by the full faith and credit of the U.S. government, which means taxpayers could be responsible for losses arising from EXIM's operations, including losses due to fraud. In fiscal year 2021, EXIM authorized more than \$5.8 billion of loan guarantees, insurance, and direct loans, according to EXIM's 2021 annual report.

To continue its operations, EXIM requires periodic reauthorization from Congress. As part of the legislation that reauthorized EXIM in December 2015, Congress included a provision for us to review the adequacy of the design and effectiveness of the controls used by EXIM to prevent, detect, and investigate fraudulent applications or loans and guarantees. It also required us to examine EXIM's compliance with the controls, including by auditing a sample of EXIM transactions within 4 years of reauthorization, and every 4 years thereafter.²

As discussed in GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework), effective fraud risk management helps to ensure that federal programs' services fulfill their intended purpose, funds are spent effectively, and assets are

¹EXIM is a wholly-owned government corporation that serves as the export credit agency of the United States, and, according to EXIM, it is intended to support financing and serve as a financier of last resort for U.S. companies that seek to sell and export their goods or services to foreign buyers and that cannot obtain private financing for their deals. EXIM is overseen by a Board of Directors, which has five members. The President of EXIM serves as the Board's Chair.

²See 12 U.S.C. § 635a-6(b), as added by the Export-Import Bank Reform Reauthorization Act of 2015, Pub. L. No. 114-94, div. E, title LI. We previously issued two reports in response to this mandate. GAO, *Export-Import Bank: EXIM Should Explore Using Available Data to Identify Applicants with Delinquent Federal Debt*, [GAO-19-337](#) (Washington, D.C.: May 23, 2019) and *Export-Import Bank: The Bank Needs to Continue to Improve Fraud Risk Management*, [GAO-18-492](#) (Washington, D.C.: July 19, 2018).

safeguarded.³ Implementing a risk-based approach to addressing potential fraud in the federal government poses a unique set of challenges to federal managers, given their programs' mission to provide the public with a broad range of critical, often time-sensitive, services, and financial assistance. As described in the Fraud Risk Framework, managers who effectively manage fraud risks develop and document an antifraud strategy that describes the program's approach for addressing the fraud risks identified during the fraud risk assessment. The purpose of proactively managing fraud risks is to facilitate, not hinder, the program's mission and strategic goals by ensuring that taxpayer dollars and government services serve their intended purposes.

The most recent legislation reauthorizing EXIM, in December 2019, added an antifraud requirement to EXIM's consideration of applications for assistance.⁴ Specifically, Section 406 of this legislation stated that EXIM shall deny an application for assistance if the end-user, borrower, lender, or exporter has been convicted of an act of fraud or corruption in connection with an application for support from EXIM made in the preceding 5 years.⁵ The legislation further states that EXIM may proceed with an application if an end-user, borrower, lender, or exporter who might be subject to the antifraud requirement can be fully excluded from the transaction.

This report focuses on EXIM's implementation of the third component of the Fraud Risk Framework and the statutory antifraud requirement. Specifically, the report assesses the extent to which EXIM has (1) designed and implemented an antifraud strategy and collaborated with stakeholders to ensure the strategy's implementation and (2) established responsibilities and designed and implemented control activities to

³GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015). More information on the Fraud Risk Framework and its leading practices, which are organized into four components, appears below.

⁴The Further Consolidated Appropriations Act, 2020 (P.L. 116-94, Div. I, title IV, 133 Stat. 2534, 3021-26, enacted December 20, 2019), extended EXIM Bank's general statutory authority for seven years, through December 31, 2026.

⁵According to EXIM, the end-user is the foreign entity that uses the U.S. goods and services. The borrower is the entity that agrees to repay the loan. The lender is the company that extends the EXIM guaranteed or insured loan to the borrower. The exporter is the U.S. entity that contracts with the buyer for the sale of the U.S. goods and services. In the case of a finance lease, if the lessor is a U.S. entity and takes title to the goods and services for lease to the foreign lessee, the lessor is the exporter.

address its statutory antifraud requirement enacted as part of its most recent authorization.

To assess the extent to which EXIM has designed and implemented an antifraud strategy and collaborated with stakeholders to ensure its implementation, we analyzed EXIM documentation and interviewed EXIM officials responsible for its development. Specifically, we reviewed EXIM's fiscal year 2021 fraud risk assessment and fraud risk profile. We analyzed the extent to which these documents and EXIM's current Antifraud Strategy aligned with relevant leading practices in GAO's Fraud Risk Framework as well as principles in the *Standards for Internal Control in the Federal Government*. The relevant leading practices from the Fraud Risk Framework relate to developing an antifraud strategy, establishing roles and responsibilities for involved in fraud risk management, and establishing collaborative relationships with stakeholders.⁶ We also reviewed documentation and information from interviews with EXIM officials on efforts to prevent, detect, and respond to fraud.

To assess the extent to which EXIM established responsibilities and designed and implemented control activities to address its statutory antifraud requirement enacted as part of its most recent authorization, we analyzed EXIM documentation and interviewed EXIM officials. Specifically, we assessed the extent to which these documents aligned with the statutory requirements and principles in *Standards for Internal Control in the Federal Government*—specifically those principles related to establishing responsibilities, designing and implementing control activities, and developing monitoring mechanisms.⁷ We also compared information on EXIM applicants and participants who should be denied under Section 406 to EXIM's participant and transaction data from

⁶We selected six of the 15 leading practices from the Fraud Risk Framework's third component that are most relevant to this objective based on a review of EXIM documents and discussions with EXIM managers responsible for fraud risk management. [GAO-15-593SP](#). GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

⁷For a full list of principles reviewed as part of this work, as outlined in GAO's *Standards for Internal Control in the Federal Government*, see appendix I.

January 1, 2020 through December 31, 2021, to identify any applicants or participants who might not have been appropriately denied.⁸

We assessed the reliability of EXIM's data by performing electronic testing on specific data elements, reviewing related documents, and interviewing knowledgeable officials responsible for the data and related information systems. We determined that the data we used in our analysis were sufficiently reliable for the purposes of our reporting objectives. For more information about our objectives, scope, and methodology, see appendix I.

We conducted this performance audit from July 2021 to September 2022 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.

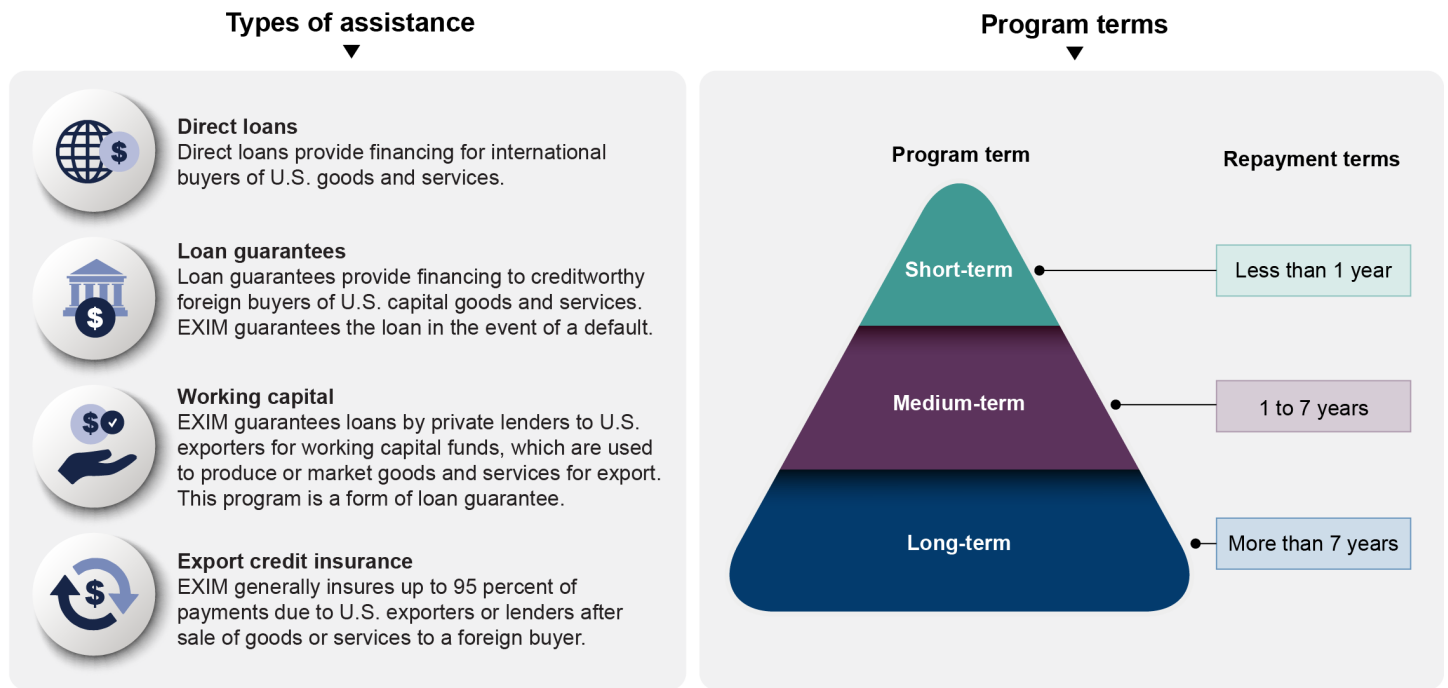
Background

EXIM Assistance and the Role of Outside Lenders

EXIM offers four major types of assistance, with products that generally have three different maturity periods. Specifically, EXIM offers direct loans, loan guarantees, export-credit insurance, and working capital guarantees. EXIM products include short-term transactions, which are for less than 1 year; medium-term transactions, which are from 1 to 7 years long; and long-term transactions, which are for more than 7 years. Figure 1 describes the types of EXIM products currently available and the associated terms of these products.

⁸According to EXIM officials, the agency considered Section 406 to be effective, and EXIM to be responsible for compliance, as soon as the legislation was passed in December 2019. Consequently, the first full month of available transaction and participant data that existed after Section 406 passed was January 2020. Therefore, we requested data beginning January 1, 2020 through December 31, 2021 - the most recent data available at the time of our review.

Figure 1: Export-Import Bank of the United States' (EXIM) Financing Programs and Program Terms



Source: EXIM. | GAO-22-105340

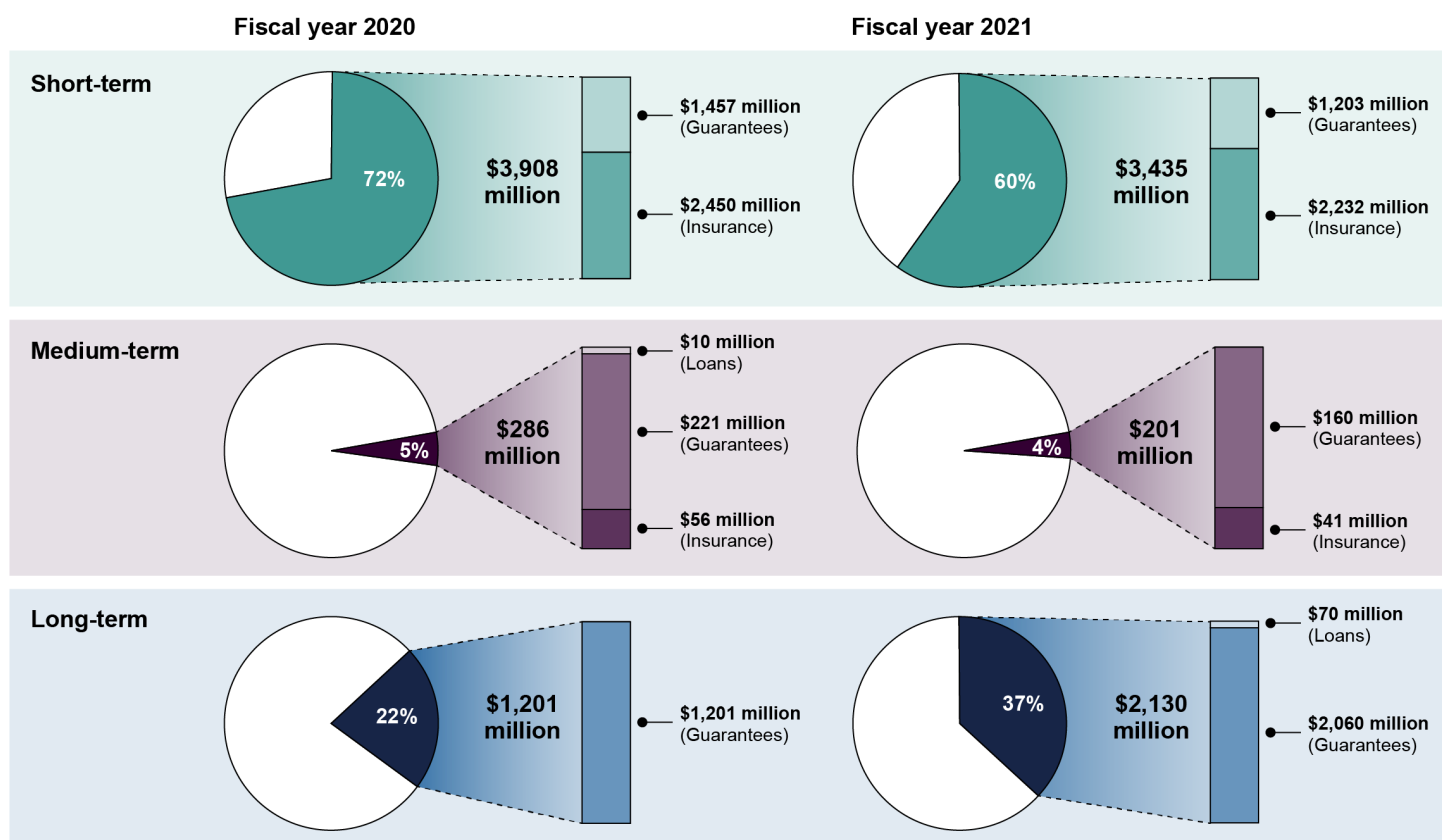
EXIM also works with outside, commercial lenders to fulfill its mission. Delegated authority lending (DAL) involves transactions that rely on underwriting by these outside lenders. In these transactions, the products handled by the outside lenders carry the same EXIM guarantees as EXIM's own offerings. Lenders with delegated authority can be found within EXIM's working capital and loan guarantee programs. DALs comprised 85 percent of all working capital transactions between fiscal years 2020 and 2021.

Additionally, brokers are other outside partners that work with EXIM in its Export Credit Insurance (ECI) program. Brokers may represent and assist insured parties in the ECI program, including insured parties with discretionary credit limits. Insured parties with discretionary credit limits are allowed to sell to various buyers, subject to the conditions of the policy.

In fiscal year 2021, EXIM authorized more than \$5.8 billion of direct loans, loan guarantees (including those for working capital), and insurance, in support of an estimated \$9.2 billion of U.S. export sales, according to

EXIM's 2021 annual report. See figure 2 below for fiscal years 2020 and 2021 authorizations by term and by program.

Figure 2: Export-Import Bank of the United States' (EXIM) Authorizations by Term and Program for Fiscal Years 2020 and 2021



Source: GAO analysis of Export-Import Bank of the United States data. | GAO-22-105340

Notes: Figure totals may not sum because of rounding. Guarantee totals include Working Capital.

Fraud Risk Management

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 (which is a function of likelihood and impact) exists when people 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. Fraud risk management is a process for ensuring program integrity by mitigating the likelihood and impact of 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.

Managers of federal programs maintain the primary responsibility for fraud risk management. The objective of fraud risk management is to ensure program integrity by continuously and strategically mitigating both the likelihood and effects of fraud. Effectively managing fraud risk helps to ensure that federal programs' services fulfill their intended purpose—that funds are spent effectively, and that assets are safeguarded.

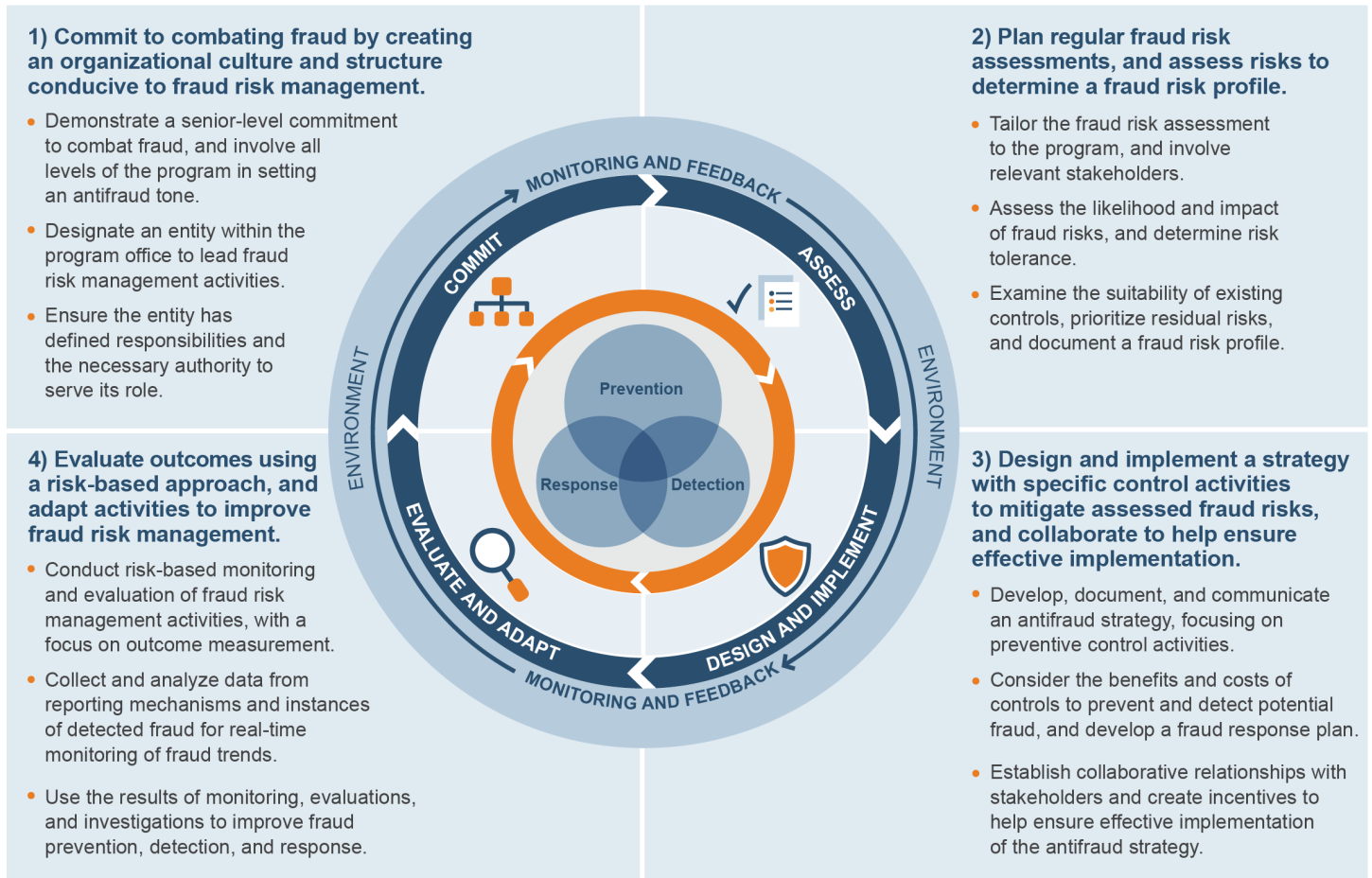
Executive branch agency managers are responsible for managing fraud risks and implementing practices for combating those risks. In July 2015, we issued the Fraud Risk Framework, which provides a comprehensive set of key components and leading practices that serve as a guide for agency managers to use when developing efforts to combat fraud in a strategic, risk-based way.⁹ The Fraud Reduction and Data Analytics Act of 2015 required 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.¹⁰ The act further required OMB to incorporate the leading practices from the Fraud Risk Framework in the guidelines. Although the Fraud Reduction and Data Analytics Act of 2015 was repealed in March 2020, the Payment Integrity Information Act of 2019 requires these guidelines to remain in effect, subject to modification by OMB as necessary, and in consultation with GAO.¹¹ As depicted below in figure 3, the Fraud Risk Framework describes leading practices within four components: 1) commit, 2) assess, 3) design and implement, and 4) evaluate and adapt.

⁹[GAO-15-593SP](#).

¹⁰Pub. L. No. 114-186, 130 Stat. 546 (2016).

¹¹Pub. L. No. 116-117, § 2(a), 134 Stat. 113, 131 - 132 (2020), codified at 31 U.S.C. § 3357.

Figure 3: The Four Components of the Fraud Risk Framework and Selected Leading Practices



Source: GAO. | GAO-22-105340

The Fraud Risk Framework includes leading practices that, if implemented appropriately, can help ensure that federal program managers, along with their stakeholders, are able to meet their responsibilities for managing fraud risks. Specifically the third component—design and implement—calls for program managers to design and implement an antifraud strategy with specific control activities to mitigate assessed fraud risks and collaborate with stakeholders to help ensure implementation. Later in this report, we discuss in detail control activities within the antifraud strategy that EXIM managers undertake to manage their fraud risks.

As discussed in the Fraud Risk Framework, the antifraud strategy is to be based on or informed by the results of the program's fraud risk assessment. Key elements of the fraud risk assessment process state that managers identify inherent fraud risks affecting the program, assess the likelihood and impact of inherent fraud risks, determine fraud risk tolerance, examine the suitability of existing fraud controls and prioritize residual fraud risks, and document the program's fraud risk profile.

- *Inherent fraud risks* are the risks that exist prior to considering management's response to those risks.
- *Risk tolerance* is the acceptable level of variation in performance relative to the achievement of objectives. In the context of fraud risk management, if the objective is to mitigate fraud risks—in general, to have a very low level of fraud—the risk tolerance reflects managers' willingness to accept a higher level of fraud risks, and it may vary depending on the circumstances of the program. A related concept is risk appetite, which describes the amount and type of risk that an organization is willing to accept in pursuit of its objectives.
- *Residual risks* are the risks that remains after inherent risks have been mitigated by existing control activities. Managers rank residual risks in order of priority and determine their responses to mitigate the likelihood and impact of residual risks that exceed their risk tolerance.
- *Fraud risk profile* is the documenting of the key findings and conclusions from the identification of fraud risks affecting the program, the assessment of the likelihood and impact of inherent fraud risks, including the risk tolerance and the prioritization of risks. The fraud risk profile is an essential piece of the overall antifraud strategy and informs the specific control activities managers design and implement within the antifraud strategy.

Effective managers of fraud risks use the program's fraud risk profile to help determine their risk responses and how to allocate resources to respond to residual fraud risks. Risk responses are actions the agency plans to take to address the fraud risk in order to bring the fraud risk within the managers' risk tolerance. The responses to fraud risks may include actions to accept, reduce, share, or avoid the risk. In general, managers accept certain risks that are within their defined risk tolerance and take one of the other three actions in response to prioritized residual fraud risks that exceed their defined risk tolerance.

Once managers have determined their risk responses, it is a leading practice for them to document an antifraud strategy based on the fraud

risk profile. The antifraud strategy describes existing fraud control activities as well as any new control activities a program may adopt to address residual fraud risks. The antifraud strategy may be agency-wide or directed at the individual program level. Effective antifraud strategies reflect the leading practices: who is responsible for fraud risk management activities, what is the program doing to manage fraud risk, when is the program implementing fraud risk management activities, where is the program focusing its fraud risk management activities, and why is fraud risk management important.

Prior and Related Work on Fraud Risk Management at EXIM

In 2018, we issued our first report on EXIM's fraud risk management efforts and found that EXIM had adopted some aspects of GAO's Fraud Risk Framework.¹² Specifically, we found that EXIM had identified a dedicated antifraud entity to lead the fraud risk management efforts and that EXIM managers and staff generally held positive views of the EXIM's antifraud culture even though their points of view on that culture differed. However, we also found the agency had not conducted a comprehensive fraud risk assessment, as provided in the framework. While EXIM took steps to compile a register of risks identified across the organization—including those related to fraud—the register did not include some known methods of fraud, such as submission of fraudulent documentation. We considered these omissions to indicate that the register was incomplete. At the conclusion of our review, EXIM said it would fully adopt GAO's Fraud Risk Framework. Officials told us at that time that they planned to complete a fraud risk assessment by December 2018 and to develop a fraud risk profile—that is, document key findings and conclusions from the assessment. As part of the July 2018 report, we made seven recommendations for EXIM's Chair and President to improve its fraud risk management activities. EXIM has implemented all seven recommendations.

Following our first report, EXIM provided us with documentation reflecting its efforts to conduct a fraud risk assessment that considered various fraud risks affecting its major financing product lines. EXIM conducted a fraud risk assessment in 2018, developed a fraud risk profile based on the assessment, and documented the fraud risk responses for each main office based on the assessment. EXIM also told us it would conduct a

¹²GAO-18-492. Within that report, we evaluated EXIM's efforts against all four components of the Fraud Risk Framework. We selected leading practices for that review based on relevancy, following discussions with EXIM managers, review of EXIM documents, and results obtained from our employee survey; as well as to describe EXIM antifraud efforts.

fraud risk assessment on a biennial basis. As a result of EXIM's 2018 fraud risk assessment, EXIM developed an antifraud strategy in 2019. EXIM next conducted a fraud risk assessment for fiscal year 2021. EXIM officials told us that the antifraud strategy developed as a result of the 2018 assessment remained the current strategy in effect following the fiscal year 2021 fraud risk assessment.

In 2019, we reported that EXIM told us it had antifraud controls in place for mitigating fraud risks that we had previously identified and communicated to EXIM officials.¹³ In that report, we reviewed more than 40 EXIM-associated court cases involving fraud and identified fraud risks involving the fraud risk factors characteristic of these cases.¹⁴ We communicated these fraud risks to EXIM officials, and they provided examples of the antifraud controls they use to help mitigate the fraud risks for their major financing products. We made two recommendations to EXIM's Chair and President that EXIM should assess and document the practicality of incorporating into its preauthorization and post-authorization character, reputational, and transaction integrity (CRTI) reviews searches for delinquent federal debts owed by applicants; and, to include if practical, implement relevant approaches—such as manual searches or batch matching. EXIM agreed with the recommendations made in our 2019 report and has fully acted on both recommendations.

¹³[GAO-19-337](#).

¹⁴[GAO-15-593SP](#). A "fraud risk factor" describes what conditions or actions are most likely to cause or increase the chances of a fraud risk occurring.

EXIM Has Designed and Implemented an Overall Antifraud Strategy and Collaborated with Stakeholders to Ensure Its Implementation, but the Strategy Is Missing Key Elements

EXIM Developed an Antifraud Strategy with Specific Control Activities to Prevent and Detect Fraud Based on a Fraud Risk Assessment and Fraud Risk Profile

The third component of the Fraud Risk Framework—design and implement—calls for federal managers to design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate with stakeholders to help ensure effective implementation. Specifically, two of the leading practices within this component state that managers should (1) use a fraud risk profile to help decide how to allocate resources to respond to residual fraud risks and (2) document an antifraud strategy that describes the program’s activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.¹⁵

EXIM’s efforts to determine risk responses and document an antifraud strategy based on a fraud risk profile generally align with these two leading practices.¹⁶ For instance, as mentioned above, EXIM documented a fraud risk profile for its three main offices that manage its assistance programs based on a fraud risk assessment. Specifically, EXIM’s Fraud Risk Oversight (FRO) team oversaw the fiscal year 2021 fraud risk assessment process for the Office of Board Authorized Finance Office of Small Business, and the Office of the Chief Management Officer. Figure 4 illustrates the roles and responsibilities of the FRO and other EXIM

¹⁵[GAO-15-593SP](#).

¹⁶As mentioned above, risk responses are actions the agency plans to take to address the fraud risk in order to bring the fraud risk within the managers’ risk tolerance.

**Fraud Risk Framework Component:
Design and Implement**

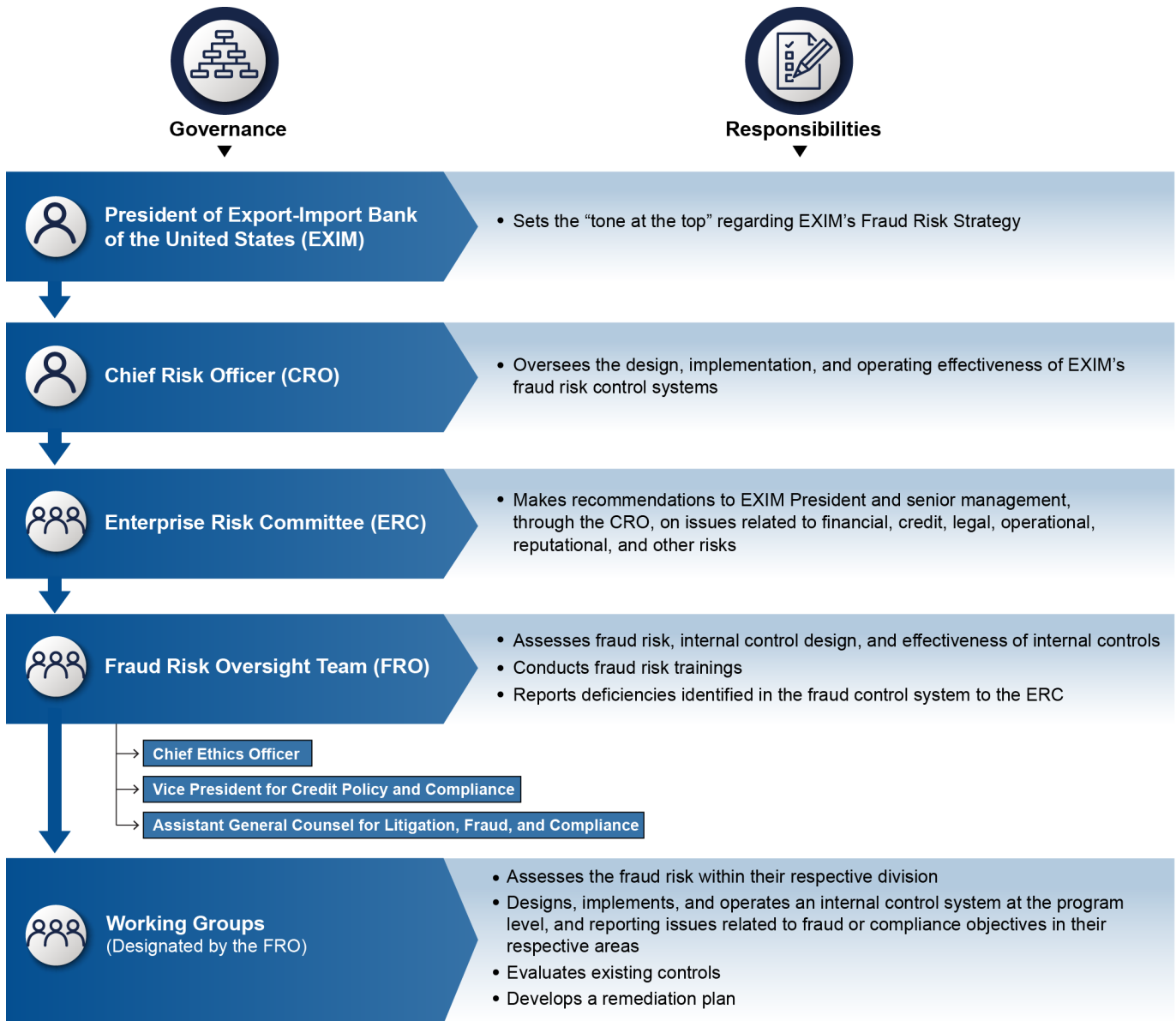
Design and implement a strategy with specific control activities to mitigate assessed fraud risks, and collaborate to help ensure effective implementation.



Source: GAO. | GAO-22-105340

entities for fraud risk management as documented within the antifraud strategy.

Figure 4: Roles and Responsibilities for Fraud Risk Management at Export-Import Bank of the United States



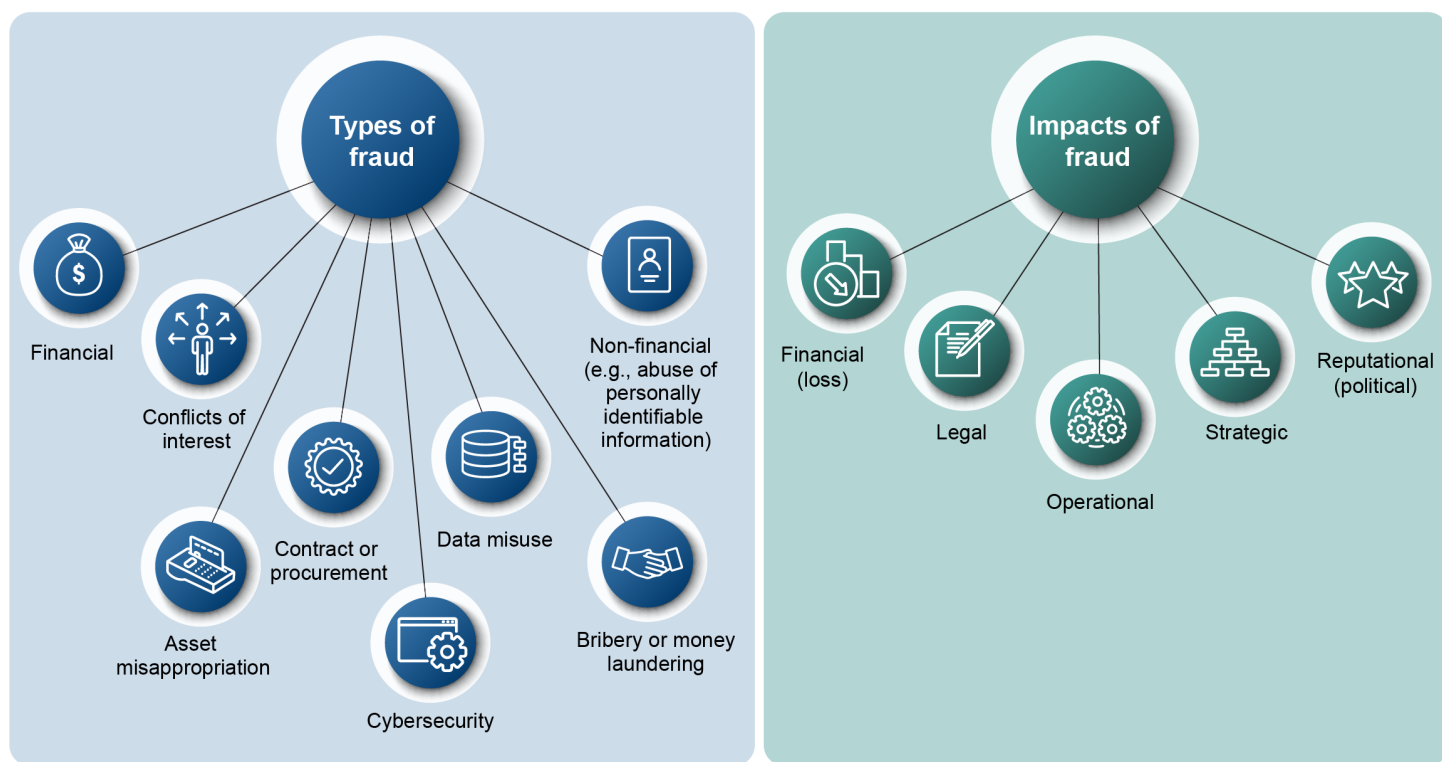
Source: GAO analysis of EXIM information and stas111/stock.adobe.com (images). | GAO-22-105340

According to EXIM’s fraud risk profile, residual risks associated with two fraud risk factors—“technology system and critical data” and “human capital management”—exceed EXIM’s stated risk appetite but were within its risk tolerance. For those risks, EXIM documented how the agency will respond, which is consistent with the leading practice of using the fraud

risk profile to help decide how to allocate resources to respond to residual fraud risks. Figure 5 shows types and impacts of potential fraud described in EXIM’s fraud risk profile.

Figure 5: Types and Impacts of Potential Fraud at Export-Import Bank of the United States (EXIM)

Types and Impacts of Potential Fraud at Export-Import Bank of the United States



Source: GAO analysis of Export-Import Bank of the United States information and stas111/stock.adobe.com (images). | GAO-22-105340

By preparing risk responses for the two fraud risk factors that exceed EXIM’s stated risk appetite—“technology system and critical data” and “human capital management”—EXIM is better positioned to prevent and detect fraud risks that exceed its risk appetite.

As mentioned above, EXIM developed an antifraud strategy in 2019 after its fraud risk assessment and decided to maintain that strategy in 2021. EXIM’s antifraud strategy describes the program’s control activities and focuses on fraud prevention; detection and response efforts; as well as monitoring and evaluation. This is consistent with the Fraud Risk Framework leading practice to document an antifraud strategy that

describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation.

Fraud Prevention. EXIM's antifraud strategy describes how EXIM's main lines of defense will help to prevent fraud. EXIM's first line of defense against fraud consists of EXIM units and staff that interact directly with the sources of fraud risk. For example, loan officers, underwriters, and their supervisors are a key part of the first line of defense against fraud in EXIM transactions. The second line of defense consists of EXIM units and staff that oversee the design, implementation, and monitoring of the fraud risk strategy and fraud risk management, including the FRO. Both the first and the second lines of defense serve to prevent fraud in EXIM transactions and operations. The third line of defense consists of independent auditors, such as the EXIM Office of the Inspector General (OIG) and GAO. For example, EXIM officials told us that case referrals to the OIG are made based on a reasonable suspicion of fraud. If something during the underwriting process raises a red flag for potential fraud, EXIM will refer it to the OIG.¹⁷ When the OIG closes a fraud referral case, it will send a close-out letter to EXIM summarizing what was done and what was found, according to EXIM officials. EXIM then reviews those letters for any new information that might warrant EXIM talking to other business units or adjusting its practices, according to officials.

Fraud awareness training is also key to fraud prevention, according to EXIM's strategy. The strategy states that EXIM will provide up-to-date awareness training on fraud, fraud risk, corruption, and integrity to all EXIM staff. EXIM also provides specific training to staff in program areas that are subject to heightened risks. For example, in 2019, EXIM provided training to one program area on fraud controls and reporting. In addition, in 2021, EXIM held trainings for all employees on fraud prevention and due diligence steps as well as training on steps EXIM employees should take to report suspicions of fraud.

Fraud Detection and Response. EXIM's antifraud strategy outlines procedures for detecting, reporting, and communicating suspected fraud. For example, according to the strategy, fraud is most often detected in EXIM transactions during the underwriting and loan approval process.

¹⁷For example, according to EXIM's antifraud strategy, one red flag is the pricing for goods or services seems to be unusually high or low.

EXIM's antifraud strategy outlines the most common ways fraud is detected:

- loan officers or underwriters discover something suspicious;
- outside whistleblowers report fraud or corruption to EXIM or to the OIG;
- claims officers discover suspicious items during the claims review process;
- EXIM collections officers, collections attorneys, and contractors discover fraud or corruption during the collections process; and
- program compliance reviews by EXIM staff reveal suspicious activity.

Once information about potential fraud or corruption is reported to EXIM's Office of the General Counsel (OGC), it is then shared with the OIG to investigate and prosecute fraud and corruption in EXIM transactions. EXIM will also disseminate information related to potential fraud or corruption to other EXIM divisions as it may be relevant to their operations.

Monitoring and Evaluation. EXIM's antifraud strategy also describes how it will monitor and evaluate fraud risk management activities. Specifically, the antifraud strategy states that ongoing monitoring will occur during regular operations. EXIM officials told us that one example of this ongoing monitoring is a biennial fraud risk survey administered to all EXIM staff.¹⁸ EXIM conducts this fraud risk survey on years between its biennial fraud risk assessments. EXIM also monitors fraud risks uncovered during its CRTI process, which involves loan officers or other EXIM officials screening applicants for indicators of fraud risk, among other things.¹⁹ According to the antifraud strategy, the scope and frequency of evaluations will depend on EXIM's fraud risk assessment results and the effectiveness of on-going monitoring procedures. EXIM officials told us that EXIM evaluates its CRTI process—an ongoing

¹⁸For example, in September 2020, EXIM surveyed staff on the question, "Who is responsible for managing fraud risk at EXIM Bank?" According to EXIM, 97 percent of survey respondents correctly replied that managing fraud risk is the responsibility of every EXIM employee.

¹⁹This CRTI process is conducted during underwriting and occurs throughout the life cycle of transactions, such as during post-authorization risk-based reviews. EXIM officials told us that, as part of this process, loan officers or other EXIM officials send the names of applicants to EXIM librarians, who perform a manual search of the Thomson Reuter's World Check database, review results, and return relevant results to EXIM officials for their consideration.

monitoring procedure—by performing reviews to ensure EXIM staff are properly screening applicants and documenting the results of their reviews, such as any indicators of fraud risk they may uncover.

By designing an antifraud strategy complete with specific control activities that focus on fraud prevention, detection, and response efforts, as well as monitoring and evaluation efforts, EXIM is better positioned to manage fraud risks and respond appropriately to instances of actual fraud.

EXIM Did Not Link Residual Risks Outlined within its Fraud Risk Profile to Its Antifraud Strategy

According to another leading practice within the third component of the Fraud Risk Framework, the antifraud strategy should demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile. This key element of the strategy helps to show where program managers are focusing their fraud risk management activities. The Fraud Risk Framework further explains that managers who effectively manage fraud risks develop and document an antifraud strategy that describes the approach for addressing prioritized fraud risks identified in the fraud risk assessment.

EXIM’s antifraud strategy does not demonstrate links between the fraud risks outlined within its fraud risk profile, including links to its highest internal and external residual fraud risks, and the antifraud strategy.²⁰ Specifically, the antifraud strategy does not mention the highest residual risk factors identified in the fiscal year 2021 fraud risk profile: “technology system and critical data” and “human capital management.”

EXIM officials told us the antifraud strategy does not detail specific risk factors that were identified in its fraud risk assessment process because the antifraud strategy is meant to be an “umbrella” document that would not contain such details. Officials told us the antifraud strategy is meant to be an overarching policy of EXIM’s fraud risk management activities and not dive down to specific risk factors. According to officials, the strategy is a living document meant to be used as policy year-after-year.

Without demonstrating links to the highest internal and external residual fraud risks outlined in EXIM’s fraud risk profile to its antifraud strategy, as called for by leading practices, EXIM is missing an opportunity to refine its antifraud strategy and ensure that it is adequately addressing risks in a dynamic risk environment. This is important because EXIM’s assessment

²⁰As mentioned above, residual risks remain after inherent risks have been mitigated by existing control activities.

of residual fraud risks has changed over time. For example, EXIM’s fiscal year 2019 fraud risk profile did not mention the fraud risk factor “human capital management.” However, the fiscal year 2021 fraud risk profile identified this fraud risk factor as having a residual risk rating that exceeded EXIM’s stated risk appetite. EXIM cannot be assured that the program’s approach appropriately addresses the prioritized fraud risks identified in the fraud risk profile following each biennial assessment. For example, the antifraud strategy could place greater emphasis on or target fraud awareness training efforts for staff to respond the fraud risk factor “human capital management.”

EXIM Established Collaborative Relationships with Internal and External Stakeholders to Help Ensure Implementation of the Antifraud Strategy

The Fraud Risk Framework states that program managers should establish collaborative relationships with stakeholders and create incentives to help ensure effective implementation of the antifraud strategy. Specifically, the third component describes leading practices for (1) establishing collaborative relationships with internal and external stakeholders to share information on fraud risks and (2) collaborating and communicating with the OIG to improve understanding of fraud risks.

EXIM established collaborative relationships with internal and external stakeholders to help implement its antifraud strategy, consistent with leading practices in the Fraud Risk Framework. For instance, EXIM established relationships with internal stakeholders, such as working groups who assist in the fraud risk assessment process. According to the antifraud strategy, working groups are teams of representatives from various EXIM divisions. The working groups are directly responsible for assessing the fraud risk within their respective divisions; designing, implementing, and operating an internal control system at the program level; and reporting issues related to fraud or compliance objectives in their respective areas, among other things.²¹

EXIM has also established relationships with its external stakeholders, including ECI partners and contractors. For example, officials told us they communicated with exporters, brokers, and other parties in the ECI program to warn them about fraud schemes that could harm them, even if the schemes do not directly harm EXIM. EXIM officials also told us that EXIM sent out notices to its broker and insured community about cybersecurity risk and cyber fraud schemes, as well as suggestions on

²¹During this review, EXIM identified working groups such as the contracting and procurement, export credit insurance, and business credit working groups, among others.

how to address these risks. In addition, EXIM shares information on how to manage fraud risk during its annual conference with external stakeholders. For example, EXIM presents “Know Your Customer” (KYC) due diligence efforts at its annual conference to external partners.²² EXIM also shares information with its contractors. For instance, according to EXIM, as a result of EXIM’s fiscal year 2019 fraud risk assessment, EXIM developed a process to share information on a weekly basis with contractors, including information on potential fraud.

Further, EXIM collaborated and communicated with its OIG to improve its understanding of fraud risks, consistent with leading practices. For example, EXIM collaborated with its OIG on antifraud training for EXIM staff and discussed mechanisms to prevent and detect fraud. EXIM’s FRO also met with the OIG to discuss mechanisms to prevent, detect, and report fraud. In addition, in summer 2021, EXIM officials met with the OIG to better understand what the OIG was doing to incorporate data analytics into their fraud risk management activities and what, if any, utility there could be for EXIM’s fraud risk management activities, according to EXIM officials.

By collaborating and communicating with stakeholders and the OIG, EXIM is well positioned to leverage these relationships to share information on emerging fraud schemes, help ensure the implementation of its antifraud strategy, and improve its understanding of fraud risks—all of which enhances its management of fraud risks.

EXIM Did Not Document Roles and Responsibilities of All External Stakeholders Responsible for Fraud Controls within Its Antifraud Strategy

According to the Fraud Risk Framework’s third component, a leading practice related to the antifraud strategy is to establish who is responsible for managing fraud risk activities. Specifically, the strategy should establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls. Further, Standards for Internal Control in the Federal Government states that management should develop and maintain documentation of its internal control system. Effective

²²According to EXIM, external parties conduct “Know Your Customer” due diligence on buyers, obligors, end-users, exporters, lenders, agents and other major transaction parties. Due diligence is conducted on transaction participants and on the transaction itself. Due diligence on transaction participants includes the review of credit and financial history, character, professional experience, and reputation. Due diligence on the transaction includes the review of all matters that may affect the likelihood of timely repayment, such as information about the goods and services being financed and related contracts, and may include review of financial projections.







documentation assists in management's design of internal control by establishing and communicating the "who, what, when, where, and why" of internal control execution to personnel.²³


EXIM's antifraud strategy documented the FRO as the dedicated antifraud entity for EXIM's fraud risk management activities. The antifraud strategy outlines the FRO's key fraud risk management activities to include overseeing EXIM's fraud risk assessment process, as well as developing and presenting fraud risk trainings to staff and external stakeholders. FRO officials told us they also oversee implementation of EXIM's antifraud controls, including the implementation of the Section 406 requirements, which are described in greater detail later in this report.

While EXIM has established that its external stakeholders have antifraud-related responsibilities, it has not documented the roles and responsibilities of all external stakeholders responsible for fraud controls within its antifraud strategy, as shown in figure 6 below.

²³[GAO-14-704G](#).

Figure 6: Export-Import Bank of the United States' (EXIM) External Stakeholders' Roles and Responsibilities for Antifraud Controls within the Antifraud Strategy

 External Stakeholder	 Roles and Responsibilities for Antifraud Controls	Roles and Responsibilities Documented within EXIM's Antifraud Strategy?
Export-Import Bank of the United States (EXIM) Office of Inspector General (OIG)	<ul style="list-style-type: none"> ▶ As an independent auditor, serves as EXIM's 3rd line of defense ▶ Investigates and prosecutes suspected instances of fraud, waste, and abuse ▶ Working with the Department of Justice, manages criminal investigations and prosecutions related to EXIM transactions and activities 	
EXIM Contractors	<ul style="list-style-type: none"> ▶ Has fraud reporting and communication responsibilities 	
EXIM Delegated Authority Lenders	<ul style="list-style-type: none"> ▶ Conducts "Know Your Customer" due diligence efforts, including exercising professional skepticism on the customer (e.g., buyers, exporters, suppliers) and the transaction ▶ Conducts due diligence to ensure it will not knowingly enter into any agreements in connection with any individual or entity that has been debarred, suspended, declared ineligible from participating in, or voluntarily excluded from participation in a covered transaction 	
EXIM Export Credit Insurance Partners (Insureds with Discretionary Credit Limits)	<ul style="list-style-type: none"> ▶ Conducts "Know Your Customer" due diligence efforts, including exercising professional skepticism on the customer and the transaction ▶ Conducts due diligence efforts to not ship to any buyer that is listed as actively excluded on the U.S. Government suspension and debarment system known the System for Award Management without prior written permission from EXIM 	

 Documented within EXIM's antifraud strategy

 Not documented within EXIM's antifraud strategy

Source: GAO analysis of EXIM information and stas111/stock.adobe.com (images). | GAO-22-105340

EXIM documented roles and responsibilities of its OIG and contractors within the antifraud strategy. For instance, EXIM documented the role of the OIG to investigate potential fraud within its strategy. According to the antifraud strategy, the OIG serves as EXIM's third line of defense and has the responsibility to investigate and prosecute instances of fraud, waste, and abuse. The strategy also states that contractors have fraud reporting and communication responsibilities.

However, the antifraud strategy does not mention or reference EXIM's DALs and ECI partners. Specifically, EXIM did not document the roles and responsibilities of EXIM's DALs and ECI partners with discretionary credit limits—such as their KYC due diligence responsibilities, which EXIM has cited as a key fraud control—within the antifraud strategy. EXIM officials told us they believe it is not necessary to document these responsibilities within its antifraud strategy because they are documented within the agreements for those external partners. These officials also told us that EXIM has posted external partners' KYC due diligence responsibilities on its website

We reviewed the Working Capital DAL master agreement and found there is no mention of their KYC due diligence responsibilities, even though these DALs conduct due diligence on the borrower, guarantor, buyer, and end-user.²⁴ EXIM officials told us that while it is true that the Working Capital DAL master agreement does not mention these lenders' KYC due diligence responsibilities, the agreement does reference a “general standard of care” that all reasonable lenders must follow. Officials also told us that they thought it would be confusing to add the KYC due diligence responsibilities to the master agreement given the fact that the due diligence processes are standard in the banking industry. These lenders are regulated entities, and bank examiners will check for KYC due diligence responsibilities during their examinations, according to officials.

By not documenting these external parties' roles and responsibilities in the antifraud strategy, EXIM is missing an opportunity to ensure that roles and responsibilities related to fraud risk management are clearly understood by all parties involved in fraud risk management.

²⁴The Working Capital DAL master agreement is officially titled the Master Guarantee Agreement. We also reviewed the medium-term DAL letter agreement and found the agreement states that lenders have KYC due diligence responsibilities. However, in January 2022, EXIM told us there were no lenders participating in EXIM's medium-term DAL program, and there were 49 lenders participating in EXIM's working capital guarantee program.

EXIM Has Established Responsibilities and Designed and Implemented Control Activities to Address Its Statutory Antifraud Requirement

EXIM Established Responsibilities to Address Its Statutory Antifraud Requirement

In implementing the Section 406 requirement, which prohibits EXIM from doing business with specific convicted parties, EXIM established roles and responsibilities consistent with standards for internal control.²⁵ For example, EXIM OGC is responsible for compiling and maintaining a Convicted Parties List (CPL), described in greater detail later in this report. For transactions approved internally, EXIM loan officers are responsible for carrying out control activities to ensure compliance.²⁶ For transactions approved externally, EXIM's DALs and ECI program participants are responsible for agreeing with their programmatic terms and conditions, which EXIM OGC updated to include the antifraud requirement. By establishing these roles and responsibilities, EXIM is better positioned to meet the antifraud requirement.

EXIM Designed and Implemented Control Activities to Address Its Statutory Antifraud Requirement

EXIM designed control activities to address the Section 406 antifraud requirement for its four major financing programs, consistent with

²⁵*Standards for Internal Control in the Federal Government* states that program managers should establish an organizational structure, assign responsibility, and delegate authority to achieve the entity's objectives.

²⁶EXIM staff, under the authority delegated by EXIM's Board of Directors, can approve smaller transactions, including those under EXIM's internal delegated authority lending resolution (separate from EXIM's external DALs).

standards for internal control.²⁷ To facilitate these control activities, EXIM created the CPL, which has two parts. Part 1 lists those individuals and companies that meet the Section 406 definition of having been convicted “in connection with an application made in the preceding 5 years.” EXIM designed a broader scope for Part 2 of the CPL based on what it believed was the intent of the Section 406 antifraud requirement. Part 2 lists those individuals, and companies known to be owned or controlled by such individuals, convicted in the preceding 5 years in connection with any EXIM matter, including the fraudulent use of EXIM’s name.²⁸ Both parts of the CPL have been made publicly available to external parties, such as DALs and ECI brokers, at the agency’s website.²⁹ As of June 2022, one individual was on Part 1 of the CPL, and 11 individuals were on Part 2 of the CPL. As part of our review, we independently verified that EXIM’s CPL was accurate and complete.³⁰

For transactions that are approved by EXIM officers,³¹ EXIM determined that its control activities for ensuring compliance with the Section 406 antifraud requirement would involve using the CPL with the existing CRTI process, illustrated in Figure 7.

²⁷*Standards for Internal Control in the Federal Government* states that program managers should design and implement control activities to achieve objectives and respond to risks. As mentioned previously, EXIM’s four major financing programs are Direct Loans, Loan Guarantees, Working Capital, and Export Credit Insurance.

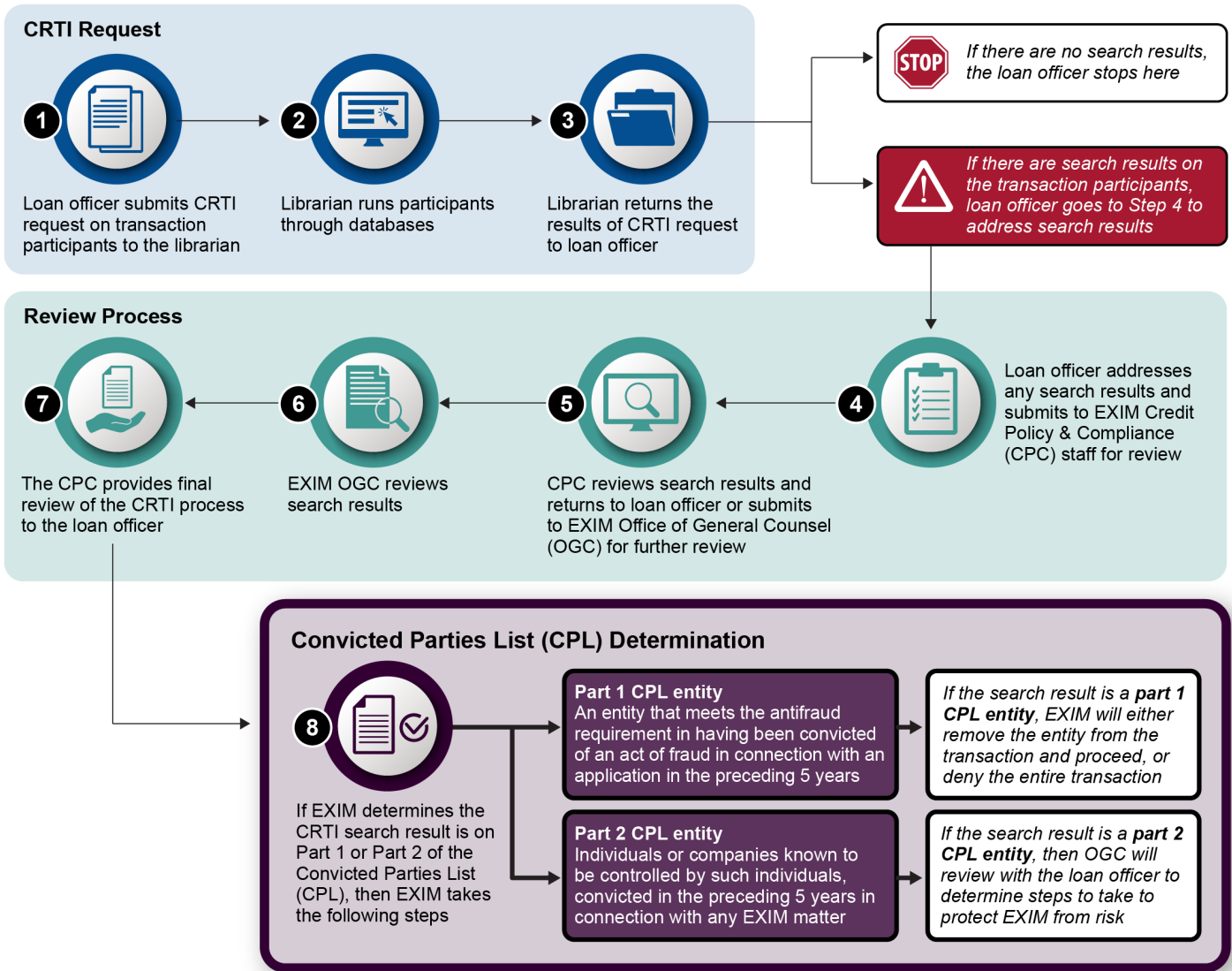
²⁸According to EXIM officials, many of the individuals on the CPL and their affiliated companies have already been administratively excluded (i.e., suspended or debarred) from participation in federal government “covered transactions,” including EXIM transactions. However, to prevent de-facto debarment, EXIM officials told us they must provide explicit permission to do business with individuals or entities on Part 2 of the CPL. De-facto debarment is when an agency excludes a potential contractor from government contracting or subcontracting without following the procedures set forth in the Federal Acquisition Regulation, which requires agencies to notify contractors of the reasons for proposed debarments and provide them with an opportunity to respond.

²⁹Additional information on the CPL appears in Appendix I. The agency website that contains the CPL is available at <https://www.exim.gov/policies/convicted-parties-list-section-406>.

³⁰For more information on how we independently verified EXIM’s CPL, see Appendix I.

³¹Transactions over \$25 million must be approved by EXIM’s board of directors. Transactions under \$25 million may be approved by other officers—such as loan officers—within EXIM.

Figure 7: Export-Import Bank of the United States' (EXIM) Character, Reputational, and Transaction Integrity (CRTI) Process Using the Convicted Parties List



Source: GAO analysis of Export-Import Bank of the United States (EXIM) information and sdecoret/stock.adobe.com (images). | GAO-22-105340

For example, when a new party is added to the CPL, EXIM verifies that CRTI will generate a search result for the convicted party when the librarian runs participants through databases, as described within step 2 of the figure above. In addition, when the CRTI review returns a search result, EXIM OGC will determine if the result is a CPL party, as described

within step 8 of the figure above. According to EXIM officials, this allows for compliance to be built directly into the existing CRTI process. There are no additional steps for loan officers to take during the process to ensure compliance with the antifraud requirement. In January 2021, EXIM OGC documented these steps within its *Procedures for Implementation of Section 406*.

For transactions approved by DALs or other external partners, EXIM implemented control activities that included updating programmatic terms and conditions to reflect the Section 406 antifraud requirement. For example, EXIM updated its Delegated Authority Letter Agreement, which directs DALs to the CPL and stipulates that DALs may not allow any buyers on Part 1 of the CPL, or any buyers on Part 2 of the CPL without obtaining EXIM's prior written consent.³² EXIM also updated its Multi-buyer Insurance Policy and Letter of Credit Policy to include statements prohibiting buyers on Part 1 of the CPL, as well as buyers on Part 2 of the CPL without obtaining EXIM's prior written consent.³³ Additionally, EXIM began requiring applicants in all of its financing programs to certify that a transaction's associated exporters, end-users, borrowers, or lenders have not been convicted of an act of fraud or corruption in connection with an EXIM application.³⁴

EXIM communicated the antifraud requirement and the updated program terms and conditions to its DALs. Specifically, in December 2021, EXIM notified all DALs via email that there was an update to their Delegated Authority Letter Agreement. The email instructed DALs to acknowledge

³²EXIM's Delegated Authority Letter Agreement contains the terms and conditions under which EXIM grants authority to an institution to guarantee a transaction, pursuant to the terms and conditions of the Master Guarantee Agreement between the lending institution and EXIM.

³³EXIM's Multi-buyer Insurance Policy states the terms and conditions under which EXIM will extend insurance to a policyholder. EXIM's Letter of Credit Policy states the terms and conditions under which EXIM provides coverage against losses caused by events such as war, revolution, and foreign exchange inconvertibility, and commercial losses caused by events such as insolvency of the foreign issuing bank, and failure to reimburse or to pay for other reasons.

³⁴As mentioned previously, according to EXIM, the end-user is the foreign entity that uses the U.S. goods and services. The borrower is the entity that agrees to repay the loan. The lender is the company that extends the EXIM guaranteed or insured loan to the borrower. The exporter is the U.S. entity that contracts with the buyer for the sale of the U.S. goods and services. In the case of a finance lease, if the lessor is a U.S. entity and takes title to the goods and services for lease to the foreign lessee, the lessor is the exporter.

the updated terms and conditions, including the antifraud requirement, by email to EXIM. As of April 2022, 48 of 49 DALs have acknowledged the new antifraud condition in their agreement.³⁵

EXIM also communicated the antifraud requirement to its ECI brokers and insureds with discretionary credit limits.³⁶ For instance, in December 2021, EXIM emailed EXIM ECI policyholders referencing the upcoming changes to their policies, including information on the CPL for insureds with discretionary credit limits. Additionally, EXIM emailed all EXIM brokers giving them final advance notice of these policy revisions. According to EXIM, these policy updates were completed by April 1, 2022.

Further, we did not identify any convicted parties in the EXIM transaction data we obtained and analyzed.³⁷ Specifically, we compared parties included on EXIM's most recent CPL, and archived versions of the CPL, to EXIM's participant and transaction data from January 1, 2020, through December 31, 2021 and found there were no matches.³⁸ EXIM officials also told us that they have not yet denied an applicant on the basis of the antifraud requirement because convicted parties are unlikely to re-apply to do business with EXIM after their conviction.

By designing and implementing these control activities, EXIM is better positioned to prevent and detect transactions with convicted parties, in

³⁵According to EXIM, the one remaining DAL that has not yet responded is currently suspended, and its delegated authority will be terminated on June 30, 2022, if it does not respond.

³⁶As mentioned above, within the Export Credit Insurance program, EXIM's brokers provide assistance to, and serve as agents for, EXIM's insured parties who hold discretionary credit limits (DCL). According to EXIM, a discretionary credit limit is a type of delegated authority allowing the exporter to sell to various buyers, subject to the conditions of their policy. Insureds with DCL are obligated to comply with Section 406. EXIM provides brokers with information about Section 406 so that they may assist their customers (insureds).

³⁷Independently identifying whether EXIM appropriately denied applications to convicted parties was outside the scope of our review.

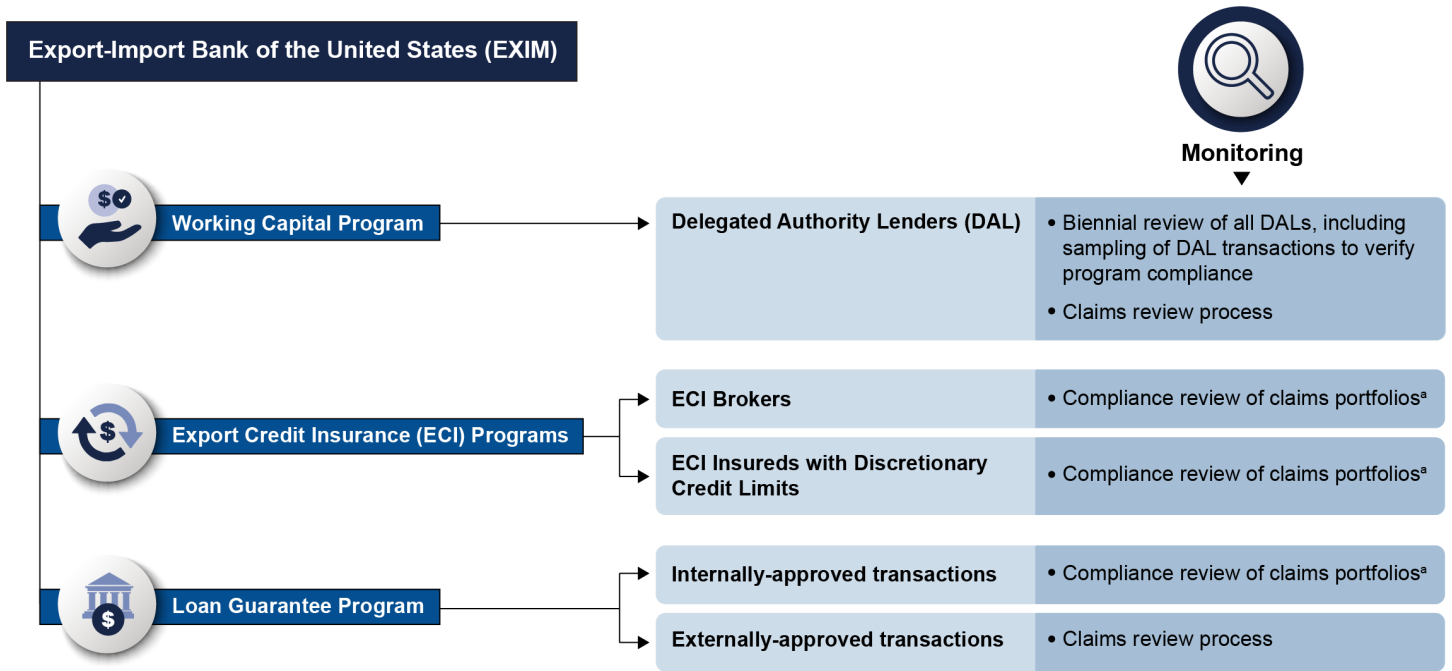
³⁸According to EXIM officials, the agency considered Section 406 to be effective, and EXIM to be responsible for compliance, as soon as the legislation was passed in December 2019. Consequently, the first full month of available transaction and participant data that existed after Section 406 passed was January 2020. Therefore, we requested data beginning January 1, 2020 through December 31, 2021—the most recent data available at the time of our review.

accordance with its Section 406 antifraud requirement, across EXIM's major financing programs.

EXIM Established Key Monitoring Procedures to Ensure Compliance with Its Statutory Antifraud Requirement

Consistent with standards for internal control, EXIM established monitoring mechanisms to comply with the Section 406 antifraud requirement.³⁹ These monitoring mechanisms apply to DALs and ECI partners, as shown in Figure 8 below.

Figure 8: Monitoring of Export-Import Bank of the United States' (EXIM) Financing Programs Section 406 Compliance



Source: GAO analysis of EXIM information and stas111/stock.adobe.com (images). | GAO-22-105340

^aEXIM is currently conducting this review and plans to complete it by the end of fiscal year 2022.

³⁹*Standards for Internal Control in the Federal Government* states that management should establish and operate monitoring activities to monitor the internal control system and evaluate the results. *Standards for Internal Control in the Federal Government* also states that management should document in policies the internal control responsibilities of the organization.

According to EXIM, the primary monitoring mechanism is EXIM's claims review process, which applies to DALs and externally-approved loan guarantees. When processing claims, EXIM can reject all or part of a claim if there is noncompliance with the programmatic conditions, including failure to meet the Section 406 antifraud requirement. Officials told us that during the claims review process, CRTI reviews consider both the claimant and the obligor.⁴⁰ If either party is found to be an entity on the CPL, EXIM can deny the claim. As mentioned above, EXIM officials told us that EXIM evaluates its CRTI process—an ongoing monitoring procedure—by performing compliance reviews to ensure EXIM staff are properly screening applicants and documenting the results of their CRTI reviews. The EXIM official who oversees the compliance review of the CRTI process told us that EXIM is currently conducting a compliance review that will include the claims portfolios. The claims portfolios include claims filed by ECI brokers, insureds, and participants in internally-approved loan guarantees. This CRTI compliance review is ongoing and is scheduled to be completed by the end of this fiscal year, according to the EXIM official. By having procedures in place for reviewing, approving, and denying claims, EXIM is better positioned to not pay claims for convicted parties in violation of federal law.

The secondary monitoring mechanism, a periodic review of transactions, is specific to EXIM DALs who approve transactions externally. During the review, EXIM plans to sample a DAL's loans and checks to ensure the DAL complied with the requirements of the program, including the antifraud requirement.⁴¹ EXIM told us they are revising the procedures to include a review for Section 406 compliance, and they anticipate completing this revision by June 30, 2022. By having a periodic review of DAL transactions, EXIM is better positioned to inform DALs about the antifraud requirement and better ensure compliance with this federal law.

Conclusions

For almost 90 years, EXIM has served as a financier of last resort for U.S. companies that seek to sell and export their goods or services to foreign buyers that cannot obtain private financing for their deals. In this role, EXIM assumes credit and country risks that the private sector is unable or unwilling to accept, including the risk of losses due to fraud. EXIM has

⁴⁰The obligor is the individual or entity who is obligated to provide a benefit or payment to another.

⁴¹Officials told us that EXIM reviews each DAL on a biennial basis (approximately once every two years).

taken a variety of actions to manage the fraud risks it faces. For example, EXIM has documented a fraud risk profile for its major lines of business.

Further, EXIM has designed an antifraud strategy with specific control activities that focus on fraud prevention, detection, and response efforts, as well as monitoring and evaluation efforts. This level of specificity in its strategy positions EXIM to manage fraud risks and respond appropriately to instances of actual fraud. EXIM also designed and implemented control activities to ensure compliance with a statutory antifraud requirement enacted in its most recent authorization. This approach will help prevent parties recently convicted of fraud or corruption against EXIM from obtaining financing from EXIM.

However, EXIM's current strategy does not contain links to its highest internal and external residual fraud risks, as called for in leading practices. Without demonstrating links to the highest internal and external residual fraud risks outlined in EXIM's fraud risk profile to its antifraud strategy, EXIM cannot be assured that it is adequately addressing risks in a dynamic risk environment or that the program's approach addresses the prioritized fraud risks identified in the fraud risk assessment. This is important because EXIM's assessment of residual fraud risks has changed over time. Additionally, EXIM's current strategy does not document the roles and responsibilities of external partners responsible for antifraud controls, such as its delegated authority lenders. By not documenting these external parties' roles and responsibilities in the antifraud strategy, EXIM is missing an opportunity to ensure that roles and responsibilities related to fraud risk management are clearly understood by all parties involved in fraud risk management.

Recommendations for Executive Action

We are making the following two recommendations to EXIM:

EXIM's Chair and President should update its antifraud strategy to demonstrate links to its highest internal and external residual fraud risks outlined in its fraud risk profile to its antifraud strategy. (Recommendation 1)

EXIM's Chair and President should update its antifraud strategy to document the roles and responsibilities of the external parties, specifically delegated authority lending (DAL) and Export Credit Insurance (ECI) partners, responsible for fraud controls. (Recommendation 2)

Agency Comments

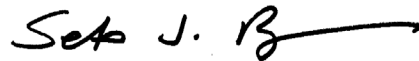
We provided a draft of this report to EXIM for review and comment. In its written comments, reproduced in appendix II, EXIM stated that it agreed

with our recommendations and described planned actions to address them. EXIM also provided technical comments, which we incorporated as appropriate.

We are sending copies of this report to the appropriate reporting congressional committees. In addition, the report will be available at no charge on the GAO website at <http://www.gao.gov>.

If you or your staff have any questions about this report, please contact me at (202) 512-4749 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 III.

Sincerely yours,

A handwritten signature in black ink that reads "Seto J. Bagdoyan" followed by a long horizontal flourish.

Seto J. Bagdoyan
Director,
Forensic Audits and Investigative Service

List of Committees

The Honorable Sherrod Brown
Chairman
The Honorable Patrick J. Toomey
Ranking Member
Committee on Banking, Housing, and Urban Affairs
United States Senate

The Honorable Christopher Coons
Chair
The Honorable Lindsey Graham
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
United States Senate

The Honorable Maxine Waters
Chairwoman
The Honorable Patrick McHenry
Ranking Member
Committee on Financial Services
House of Representatives

The Honorable Barbara Lee
Chairwoman
The Honorable Hal Rogers
Ranking Member
Subcommittee on State, Foreign Operations, and Related Programs
Committee on Appropriations
House of Representatives

Appendix I: Objectives, Scope, and Methodology

This report assesses the extent to which the Export-Import Bank of the United States (EXIM) has (1) designed and implemented an antifraud strategy and collaborated with stakeholders to ensure the strategy's implementation; and (2) established responsibilities and designed and implemented control activities to address its statutory antifraud requirement enacted as part of its most recent authorization.

As part of this work, we determined that internal controls were significant to our objectives. Specifically, the control environment component of internal control, along with the related principle that management should establish structure, responsibility, and authority to achieve organizational objectives, as outlined in the *Standards for Internal Control in the Federal Government*, was significant to our objectives.¹ Additionally, the control activities component of internal control, along with the principles that management should (1) design control activities to achieve objectives and respond to risks, (2) implement control activities through policies and procedures, (3) use quality information, and (4) communicate internally and externally, were significant to our objectives. Finally, the monitoring component of internal control, along with the principle that management should perform monitoring activities, was also significant to our objectives. To assess the control activities in both objectives, we analyzed relevant program and organizational documentation, reviewed relevant federal laws, interviewed EXIM officials, and reviewed EXIM transaction data.

To assess the extent to which EXIM has designed and implemented an antifraud strategy and collaborated with stakeholders to ensure its implementation, we analyzed EXIM documentation and interviewed EXIM officials responsible for its development. Specifically, we reviewed EXIM's fiscal year 2021 fraud risk assessment and fraud risk profile. We also reviewed EXIM's 2019 Antifraud Strategy—the current strategy in place. We analyzed the extent to which these documents and EXIM's Antifraud Strategy aligned with leading practices in the third component of GAO's *A Framework for Managing Fraud Risks in Federal Programs* (Fraud Risk Framework) and *Standards for Internal Control in the Federal Government*.²

¹GAO, *Standards for Internal Control in the Federal Government*, [GAO-14-704G](#) (Washington, D.C.: Sept. 10, 2014).

²GAO, *A Framework for Managing Fraud Risks in Federal Programs*, [GAO-15-593SP](#) (Washington, D.C.: July 28, 2015) and [GAO-14-704G](#).

The Fraud Risk Framework's third component describes 15 leading practices for designing and implementing an antifraud strategy and establishing collaborative relationships with internal and external stakeholders. From those 15 leading practices, we selected six that are most relevant to this objective, such as those on developing, documenting, and communicating an antifraud strategy based on a review of EXIM documents and discussions with EXIM managers responsible for fraud risk management. The six selected leading practices are

1. use the fraud risk profile to help decide how to allocate resources to respond to residual fraud risks;
2. develop, document, and communicate an antifraud strategy to employees and stakeholders that describes the program's activities for preventing, detecting, and responding to fraud, as well as monitoring and evaluation;
3. establish roles and responsibilities of those involved in fraud risk management activities, such as the antifraud entity and external parties responsible for fraud controls, and communicate the role of the Office of Inspector General (OIG) to investigate potential fraud;
4. demonstrate links to the highest internal and external residual fraud risks outlined in the fraud risk profile;
5. establish collaborative relationships with internal and external stakeholders, including other offices within the agency; federal, state, and local agencies; private-sector partners; law-enforcement entities; and entities responsible for control activities to, among other things, share information on fraud risks and emerging fraud schemes, and share lessons learned related to fraud control activities; and,
6. collaborate and communicate with the OIG to improve understanding of fraud risks and align efforts to address fraud.

We assessed the extent to which these documents aligned with selected principles *in Standards for Internal Control in the Federal Government* for documenting the internal control system. We also reviewed documentation and information from interviews with EXIM officials on EXIM's efforts to prevent, detect, and respond to fraud.

To assess the extent to which EXIM established responsibilities and designed and implemented control activities to address its statutory antifraud requirement enacted as part of its most recent authorization, we analyzed EXIM documentation, such as policy and procedures

documentation related to the Section 406 requirement, and interviewed EXIM officials.³ Specifically, we assessed the extent to which these documents aligned with selected principles *in Standards for Internal Control in the Federal Government* that we determined to be significant to our objectives, as described earlier in this appendix.

We also compared information on EXIM applicants and participants who should be denied under Section 406 to EXIM's participant and transaction data from January 1, 2020 through December 31, 2021, to identify any applicants or participants who might not have been appropriately denied.⁴ As part of this work, we

1. assessed the design and implementation of EXIM's control activities for Section 406 compliance against relevant federal internal control standards,
2. independently verified the accuracy and completeness of EXIM's Convicted Parties List (CPL);⁵ and,
3. conducted an independent comparative data analysis to determine whether individuals on the CPL appear in the EXIM transaction data.

As part of this work, we obtained EXIM's CPL as of January 2022, and archived versions of the CPL that date back to September 2021. EXIM's

³The Further Consolidated Appropriations Act, 2020 (P.L. 116-94, Div. I, title IV, 133 Stat. 2534, 3021-26, enacted December 20, 2019), extended EXIM Bank's general statutory authority for seven years, through December 31, 2026. Section 406 of the Act requires EXIM to deny an application if the end-user, borrower, lender, or exporter has been convicted of an act of fraud in connection with an EXIM application in the preceding 5 years.

⁴According to EXIM officials, the agency considered Section 406 to be effective, and EXIM to be responsible for compliance, as soon as the legislation was passed in December 2019. Consequently, the first full month of available transaction and participant data that existed after Section 406 passed was January 2020. Therefore, we requested data beginning January 1, 2020 through December 31, 2021 - the most recent data available at the time of our review.

⁵The Convicted Parties List contains the names of individuals convicted of an act of fraud or corruption in connection with an EXIM application in the preceding 5 years. EXIM maintains this list at <https://www.exim.gov/policies/convicted-parties-list-section-406> as "Part 1." EXIM also compiles a list of "Part 2" individuals/associated entities. Part 2 individuals were convicted in the preceding 5 years in any matter that has a connection with EXIM and are therefore not necessarily denied under Section 406. However, EXIM's express written permission is required before proceeding with an EXIM-supported transaction in which any individual or company listed under Part 2 is a buyer, borrower, end-user, lender, or exporter.

CPL changes over time as new people are convicted and formerly convicted individuals exceed the 5-year prohibition timeframe. EXIM updates the CPL by manually adding new parties to the CPL as they are convicted, and the CPL automatically drops parties that were convicted more than five years prior.⁶

To independently verify the completeness and accuracy of the list, we used available resources to locate cases that resulted in conviction for fraud or corruption related to an application made to EXIM including undertaking a docket search on WestLaw Edge. Using this database, we searched for criminal cases filed after January 1, 2015 that had the keywords “Export-Import” or “EXIM” or “EX-IM.” The search returned 16 results, none of which related to the Export-Import Bank of the United States. Instead, these unrelated cases had charges related to smuggling items or failing to report export/import monetary instruments.

Using the “Department of Justice News Releases” within WestLaw Edge, we also searched for “Export-Import Bank” for press releases after 2012, and there were 20 results. We did not find any convicted parties that were included on the EXIM’s list posted as of February 24, 2022.

We assessed the reliability of EXIM’s data by performing electronic testing on specific data elements, reviewing related documents, and interviewing knowledgeable officials responsible for the data and related information systems. We determined that the data we used in our analysis were sufficiently reliable for the purposes of our reporting objectives.

We conducted this performance audit from July 2021 to September 2022 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.

⁶According to EXIM officials, EXIM becomes aware of newly convicted parties from Department of Justice press releases and the EXIM OIG’s Office of Investigations, and its procedures for adding new individuals or entities to the CPL are documented.

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



Reducing Risk. Unleashing Opportunity.

August 30, 2022

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

Re: GAO Report “Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts” (GAO-22-105340)

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, “Additional Documentation about Stakeholder Roles and Clarity about Fraud Risks Would Strengthen Antifraud Efforts” (GAO-22-105340). 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 the GAO.

The GAO has been mandated since 2015 to periodically review EXIM antifraud controls. EXIM has instituted robust antifraud controls and implemented all prior GAO recommendations from prior reviews. We appreciate the GAO recognizing in this report that EXIM “established responsibilities and designed and implemented control activities to address its antifraud requirement, as required by its authorizing legislation.” Further, EXIM is pleased that GAO’s analysis of EXIM 2020-2021 transaction data to “determine if EXIM had appropriately denied applications by parties convicted of EXIM-related fraud or corruption charges ... did not identify any relevant convicted parties within the EXIM transaction data.”

The GAO has made two recommendations in this report to strengthen EXIM antifraud efforts. The Bank concurs with both recommendations and will move forward with implementing the recommendations.

Recommendation 1: EXIM’s Chair and President should update its antifraud strategy to demonstrate links to its highest internal and external residual fraud risks outlined in its fraud profile to its antifraud strategy.

Management Response: EXIM concurs with the recommendation and will ensure that the fraud risk strategy is updated to highlight that the fraud risk profile, which can change with each fraud risk assessment, will be duly noted to allow for the appropriate management focus.

1

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



Reducing Risk. Unleashing Opportunity.

Recommendation 2: EXIM’s Chair and President should update its antifraud strategy to document roles and responsibilities of the external parties, specifically Delegated Authority Lending (DAL) and Export Credit Insurance (EC) partners responsible for fraud control.

Management Response: EXIM concurs with the recommendation and will update its antifraud strategy.

EXIM is committed to the continuous improvement of its processes to reduce, mitigate, and eliminate fraud and hold accountable those who attempt to defraud the U.S. government. We look forward to strengthening our working relationship and continuing to work closely with the GAO.

Sincerely,

**ADAM
MARTINEZ** Digitally signed by
ADAM MARTINEZ
Date: 2022.08.30
11:41:30 -04'00'

Adam Martinez
Chief Management Officer
Export-Import Bank of the United States

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Seto J. Bagdoyan at (202) 512-4749, BagdoyanS@gao.gov

Staff Acknowledgments

In addition to the contact named above, Jonathon Oldmixon (Assistant Director), Isabelle Aboaf, Carla Craddock, David Dornisch, Paulissa Earl, Colin Fallon, James Healy, Andrew Kincare, Michael Maslowski, Maria McMullen, and Sabrina Streagle made key contributions to this report.

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 our website. Each weekday afternoon, GAO posts on its [website](#) newly released reports, testimony, and correspondence. You can also [subscribe](#) to GAO's email updates to receive notification of newly posted products.

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 [Email 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 FraudNet:

Website: <https://www.gao.gov/about/what-gao-does/fraudnet>

Automated answering system: (800) 424-5454 or (202) 512-7700

Congressional Relations

A. Nicole Clowers, Managing Director, ClowersA@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

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

