Program Integrity: The Antifraud Playbook

You can invest years in building your agency's reputation and public trust in it, and one incident of fraud can destroy it. The American people expect agencies to protect their tax dollars by developing and maintaining governance structures, controls, and processes to safeguard resources and assets. By making the management of fraud risk a priority at your agency, you can balance the achievement of your agency's mission with enhanced program integrity.

* * *

How much does your agency lose annually in fraud? It is probably significantly higher than you think. The deceptive nature of fraud makes it extremely difficult to quantify because it is invisible until you discover it.

* * *

This playbook provides a four-phased approach with 16 plays drawn from successful practices from the federal government and private sector to help you combat the risk of fraud at your agency. Combating government fraud is an ongoing challenge, but this playbook will provide you with practical and actionable guidance to help you in your antifraud journey.

See the Plays

Help Improve This Content

Introduction

What is program integrity and why is it important?

The term "program integrity" encompasses the concept that programs should be organizationally and structurally sound and capable of achieving their mission without compromise. It is the umbrella under which payment integrity, internal controls, fraud risk management, and improper payments prevention fall.

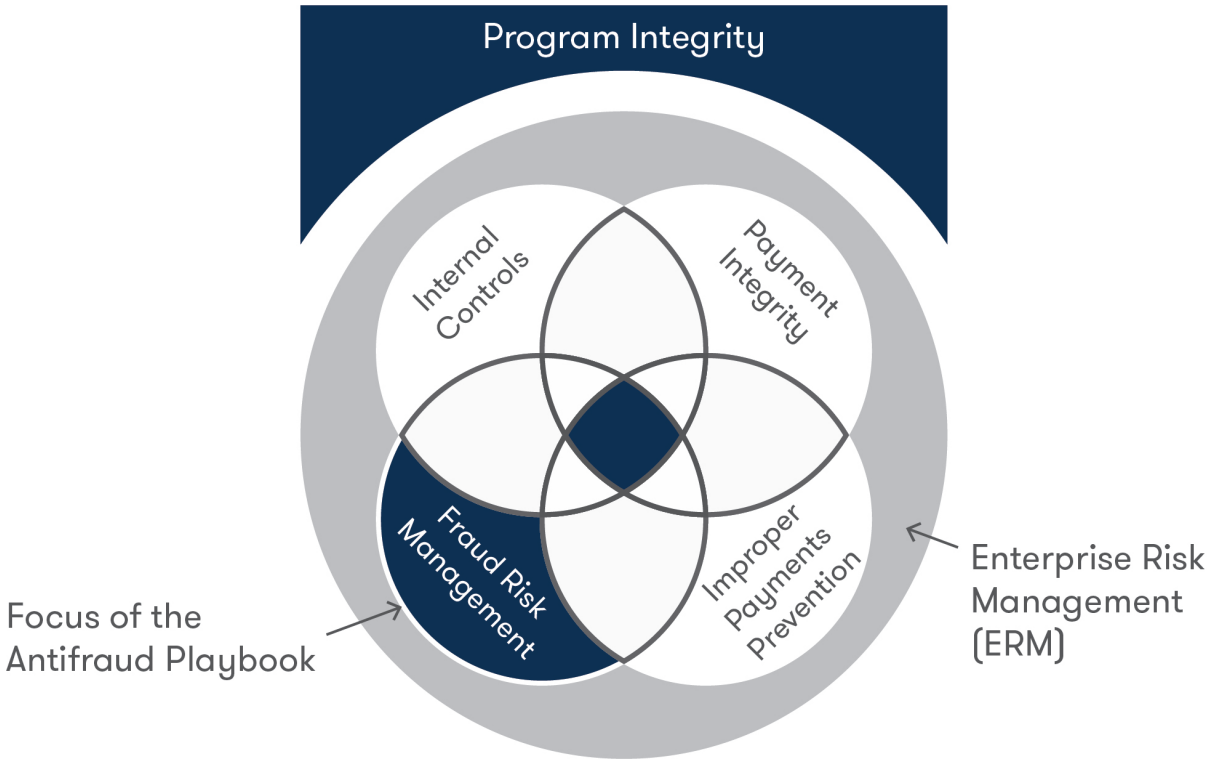


Figure 1: Program Integrity

Program integrity is a foundational concept that seeks to ensure that agencies develop and maintain governance structures, controls, and processes to safeguard taxpayer resources. As shown in figure 1, program integrity is a broad concept with numerous components, including fraud risk management. This playbook focuses on fraud risk management, but it is important to consider how a fraud risk management program connects with other components of your program integrity effort, including internal controls, improper payments prevention, and ERM.

What constitutes fraud vs. fraud risk? Why is managing fraud risk important?

There are a lot of definitions floating around for what constitutes an incident of fraud. Most agree that the word fraud denotes an event that has been investigated and successfully prosecuted, with criminal intent proven in a court of law. The Government Accountability Office (GAO) Standards for Internal Control in the Federal Government (the Green Book) defines Fraud as obtaining something of value through willful misrepresentation.

However, for the purposes of fraud risk management, the important thing to consider is whether your agency has vulnerabilities within its processes and controls that could be exploited to obtain something of value through willful misrepresentation. For the purposes of this playbook, *fraud risk* is defined as:

- The vulnerability that an agency faces from individuals capable of combining all three elements of the fraud triangle, deriving from sources either internal or external to the organization.

Note: For further discussion on the Fraud Triangle, see the 'Fraud Triangle: Quick Tip!' in Play 5 below.

When considering your risks to fraud, whether or not a fraudster will be convicted is less important than ensuring weak controls are strengthened in order to eliminate the fraud vulnerabilities. Proactive fraud risk management is a process of identifying and mitigating fraud risks. For example, you don't wait until you're robbed to decide that you should lock your doors. If there have been recent crimes in the neighborhood, the *likelihood* is higher that you'll get robbed. If you have valuables or no insurance, the *impact* is higher. If the robber evades conviction, you don't reconsider the robbery as an accidental loss of some kind.

How was this playbook developed?

This playbook represents compiled information related to best practices and lessons learned surrounding the development and advancement of antifraud efforts within various agencies. It draws on the insights of a wide range of agency officials responsible for designing or managing antifraud and integrity-focused programs. We compiled this information and combined it with private sector and industry best practices to build out each play within this playbook.

Why was this playbook developed?

The 16 plays that follow provide practical guidance for government agencies looking to develop antifraud programs or mature existing antifraud activities. The playbook was also developed to help clarify and operationalize the concepts put forward in other guidance in order to help your agency adopt the practices within that guidance.

Overall, the playbook offers guidance on how to proactively manage fraud risk in order to prevent fraud within agencies. While the playbook is not meant to provide an exhaustive list of fraud risk management activities, it will help you start building a robust antifraud program and exemplifies our first piece of advice—just do something, start somewhere.

How is the playbook organized?

The playbook includes 16 plays, which are organized into the following four phases:

1. **Create a Culture**—Build a culture that is conducive to both integrity efforts and furthering antifraud measures at your agency.
2. **Identify and Assess**—Identify your fraud risks and develop a path forward for executing, repeating, and expanding a fraud risk assessment that is unique and customizable for your agency.
3. **Prevent and Detect**—Develop or strengthen antifraud controls that mitigate your highest risk areas and start or advance your fraud analytics program.
4. **Insight into Actions**—Use available information, either within your agency, or from external sources, and turn that insight into actionable tasks.

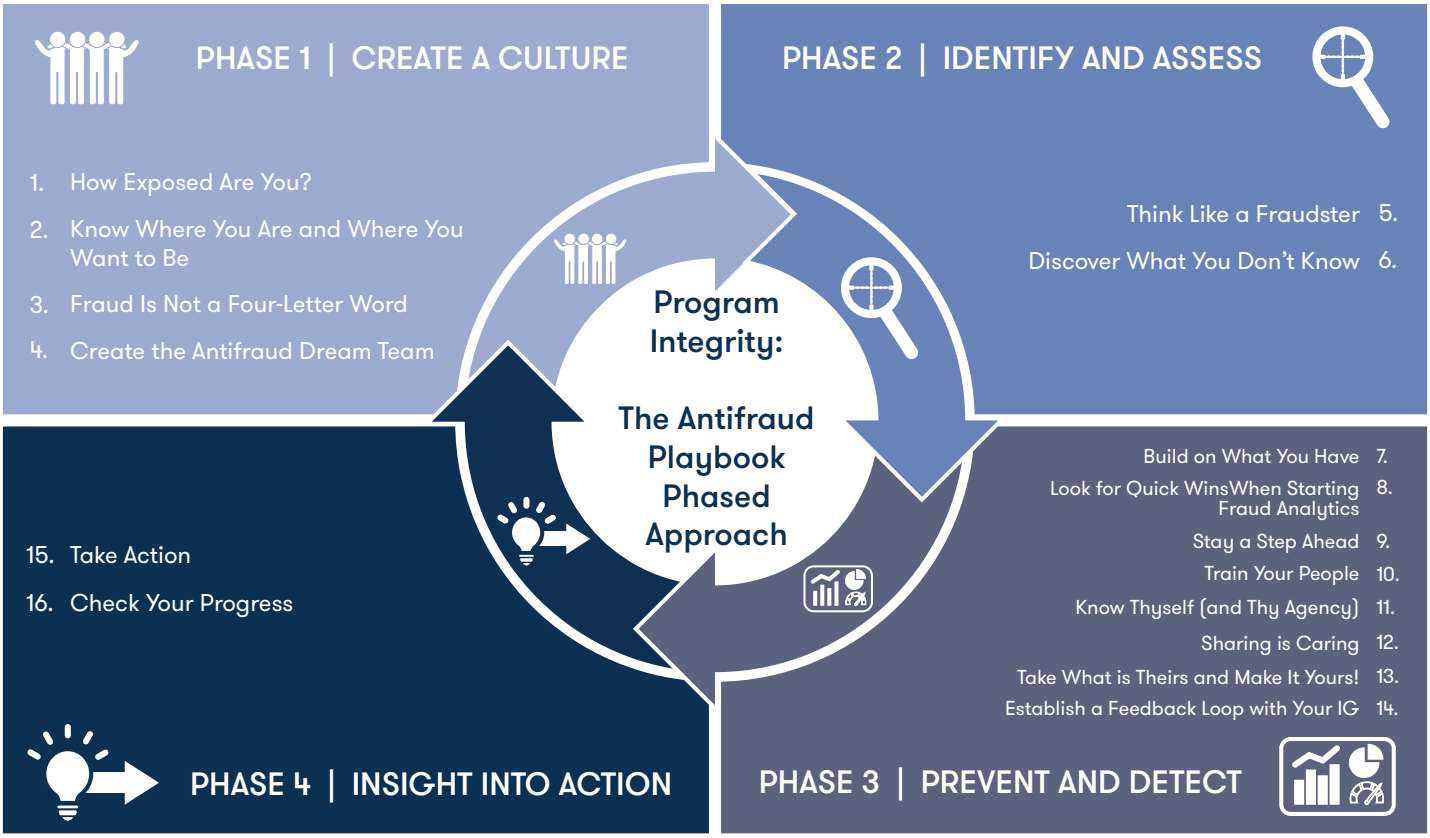


Figure 2: Four-Phased Approach

Overall, the plays have a similar format and structure. Within each play there are a series of elements that may be present including: why is this important, key points, tables, case studies, checklists, quotes, examples, and call-outs. Each play contains unique content so not every play contains every element. For example, some plays may have a case study while other plays may have an illustration, while some plays will have neither.

How can I use the playbook?

There are many ways you can use this playbook. At a summary level, here are some things to consider:

The playbook can and should be used as it best fits your needs.
You do not have to implement the playbook as written. This is not a compliance checklist, but rather a compilation of information to help you achieve success in your antifraud initiatives. You are free to select the plays that are more useful or feasible for your agency. For example, if you have limited resources and are unable to conduct a fraud risk assessment across your entire agency (see *Play 6*), then you can instead choose to pilot a fraud risk assessment on a particular program or function, such as travel and purchase cards.

You do not have to implement the playbook sequentially, or in its entirety.
You are free to pick and choose the plays that will bring the most value to your agency. Or you can pick and choose the plays you are able to implement with the resources your currently have available. That said, we do recommend that every agency conduct a fraud risk assessment, both to adhere to GAO's *Framework for Managing Fraud Risks in Federal Programs* (GAO's Fraud Risk Framework) and to focus antifraud efforts on the highest fraud risks.

You can utilize the playbook differently based on your level of maturity.
If your antifraud efforts and program are just beginning, don't worry. The playbook is organized in such a way that each phase builds on the previous one, leading to a robust program integrity and antifraud program at the finish line. If your antifraud program is more mature, this playbook will help you continue to advance your initiatives. We encourage you to jump to the plays most pertinent to your agency's current efforts, priorities, and strategic goals.

No matter how you use this playbook, there is valuable information and guidance provided to help you develop or advance your program integrity and antifraud programs.

How does the playbook align to relevant guidance?

The playbook helps to clarify and operationalize the concepts put forward in other guidance, including GAO's Fraud Risk Framework, GAO's Green Book, Fraud Reduction and Data Analytics Act of 2015, improper-payment legislation, and the Office of Management and Budget (OMB) circulars. Additionally, the playbook offers suggestions for integrating disparate compliance activities using your existing governance structure.

See *Appendix A* for further details.

What other resources are out there?

The playbook is not intended to be all-inclusive, and is not the only resource available. We have identified additional publicly available resources that provide valuable information on fraud awareness, prevention and detection activities, and related best practices. Agencies should use these resources in conjunction with the playbook when developing, implementing, or advancing your antifraud programs. See *Appendix D* for further details.

The Plays

Create a Culture

1. How Exposed Are You?
2. Know Where You Are and Where You Want to Be
3. Fraud is Not a Four-Letter Word
4. Create the Antifraud Dream Team

Identify and Assess

5. Think Like a Fraudster
6. Discover What You Don't Know

Prevent and Detect

7. Build on What You Have
8. Look for Quick Wins When Starting Fraud Analytics
9. Stay a Step Ahead
10. Train Your People
11. Know Thyself (and Thy Agency)
12. Sharing is Caring
13. Take What is Theirs and Make It Yours!
14. Establish a Feedback Loop with Your IG

Insight into Action

15. Take Action
16. Check Your Progress

Create a Culture

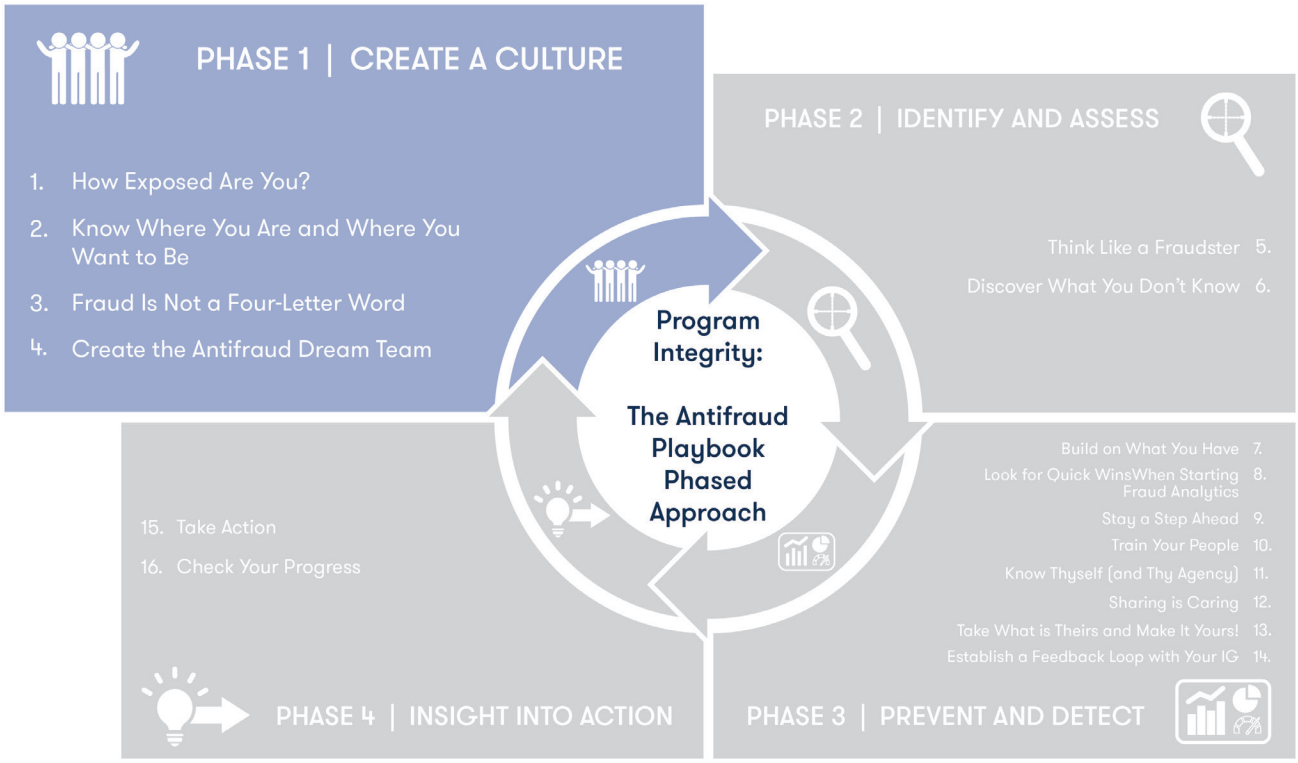


Figure 3: Four-Phased Approach, Create a Culture

Why is this important

The first phase in your antifraud journey is all about building a structure and developing a culture to combat fraud at all levels of your agency. A fraud-aware culture is a key component of every antifraud program, and can even act as a preventive measure for combating fraud at your agency. Building a structure is a key component to achieving a fraud-aware culture. Plays 1 and 2 are aimed to help you begin that process. These plays focus on helping you gain insight related to your agency's fraud exposure, identifying your current level of maturity, and mapping a path forward.

The remaining plays help focus attention on antifraud through fraud-awareness initiatives (*Play 3*) and by forming a dedicated entity to lead your agency's fraud risk management activities (*Play 4*).

Overall, the four plays included in this phase will help you build a culture that is conducive to antifraud efforts and furthering antifraud measures at your agency.

What plays are included

1. How Exposed are You?
2. Know Where You Are and Where You Want to Be
3. Fraud Is Not a Four Letter Word
4. Create the Antifraud Dream Team

Play 1 - How Exposed Are You?

Why is this important

Not every agency needs the same level of effort when it comes to an antifraud program. The first step in determining the scope of your antifraud effort is to understand how vulnerable your agency is to fraud—i.e., your "fraud exposure." The "fraud exposure" should be a high-level identification of the major types of fraud risks that exist in the agency and the programs that are most susceptible to those risks. This approach can help narrow the focus of your fraud risk assessment to those programs that are both at greatest risk and involve factors that are most vulnerable to fraud. Those agencies with a higher "fraud exposure" will need to invest more in developing a robust antifraud program than those with low fraud exposure. After understanding your level of fraud exposure you can develop a fraud risk management approach that is appropriate for your agency's unique needs and vulnerabilities. This may not be perfect and will change as your fraud risk management efforts evolve. Use this to help focus your first steps and not as the final result of your fraud risk management efforts.

KEY POINTS

- **Determining your fraud exposure is a method for understanding the inherent vulnerabilities your agency faces** based on how it's structured and how it interacts with third parties.

  For example, if your agency does not make any benefit payments, doesn't administer any grant or loan programs, and has limited interaction with third parties, such as vendors and contractors, your fraud exposure is likely low and would relate primarily to internal fraud, such as payroll, travel, and purchase card fraud.

Play 1 - How Exposed Are You?

KEY POINTS (continued)

- **Outline the factors that contribute to fraud risk areas** such as: the "materiality" or financial significance of a program; how much you rely on self-reported information; how well your agency has complied with existing regulations; and the results of past Inspector General (IG) or GAO audits, among others.
- **Think about financial and non-financial risks as well as the effects on your agency's reputation.** For example, compromising the security of personally identifiable information (PII) can be just as damaging as making payments to a fraudster. The payment has a financial impact while the compromised PII will negatively affect your reputation. Consider what affects your agency's bottom line and customers, along with what will land your agency on the cover of the Washington Post.
- **Quantify the risk factors to determine an overall "fraud exposure"** (see these *Tables* for guidance).
- **The fraud exposure determination is not meant to be an exhaustive risk assessment**—it is supposed to help you quickly understand the level of fraud your agency and programs may be susceptible to so you can better tailor your antifraud strategy.

Fraud Exposure Tables

The following examples (*Table 1* and *Table 2*) demonstrate some common elements that comprise a fraud exposure determination. The tables provide a simple methodology for determining risk factors (horizontal axis) within different hypothetical federal programs (vertical axis). **For this example, each of the risk factors carries a weight of 25% to contribute to the total fraud exposure. Keep in mind that these weights do not have to be equal (though the weights should all add up to 100%) and they can and should be tailored from agency to agency or from program to program to reflect the priority and relevancy of the risk factors to the program or organization. The factors may vary for financial and non-financial programs.** The total fraud exposure is a combination of the preceding factors within a given program.

Play 1 - How Exposed Are You?

Fraud Exposure Tables (continued)

When looking at improper payments, agencies have guidance on what constitutes a high risk program. For the management of fraud risks, this guidance does not exist; it is up to you and your colleagues to understand and decide the thresholds for these risk factors according to the needs and priorities of your program or agency. The following examples determined that an agency that had to verify more than half of the external information coming to it was putting itself at a high risk of fraud. Similarly, the examples state that a bank transfer of funds is less risky than issuing an Electronic Benefit Transfer (EBT) card or cash, with each of the three forms of payment having different risk levels. These determinations are for example purposes only.

	QUANTITATIVE FACTORS	QUALITATIVE FACTORS			
	Program outlays compared to those of other agency programs	*Payment Type*	*Payment or benefit recipient*	*Amount of external information to verify*	*Fraud exposure*
Risk Factor Weight	25%	25%	25%	25%	
Loan program 1	Highest quintile - High Risk	Bank Transfer - Low Risk	Registered Institution - Low Risk	Less than 10% - Low Risk	**Low-Medium**
Loan program 2	Lowest quintile - Low Risk	Cash - High Risk	Individual - High Risk	Greater than 50% - High Risk	**Medium-High**
Loan program 3	Middle three quintiles - Medium Risk	EBT card - Medium Risk	University faculty member - Medium Risk	10% - 50% - Medium Risk	**Medium**

Table 1: Fraud Exposure Scenario A

	Amount of external information to verify	*Information source (domestic or international)*	*Information source (electronic or paper)*	*History of applicant*	*Fraud exposure rate*
Risk Factor Weight	25%	25%	25%	25%	**100%**
Work Visa	Greater than 50% - High Risk	Domestic - Low Risk	Paper - High Risk	Previously denied - High Risk	**Medium-High**
Lost Passport Application	Less than 10% - Low Risk	International - High Risk	Electronic - Low Risk	First lost passport - Low Risk	**Medium-Low**

Table 2: Fraud Exposure Scenario B

Table Note: The figures and corresponding risk determinations in this table are for example purposes only. Actual figures will vary based on the program and agency.

Play 1 - How Exposed Are You?

These tables can help identify areas of concern, but what do you do when your programs end up with the same fraud exposure and you can only focus on one? In that event it may be prudent to identify which program has the larger budget impact or larger impact on operations and identify solutions for that program.

In order to help you build your own table to determine your fraud exposure, below are some examples of program types and relevant risk factors. This is not an exhaustive or comprehensive list but a few examples to help you get started and brainstorm other risk factors relevant to your agency or program. Additionally, factors for one type of program can apply to multiple program types even if they aren't listed here.

Grant, Loan, Reimbursement and Benefit Programs

- Size of payments as a percentage of all payments
- Type of payment (cash, transfer of funds, EBT, etc.)
- Recipient (institution, individual, etc.)
- Amount of information to be verified
- Program history
- Turnover of key staff
- Amount of PII handled

Contracting

- Vendor history
- Contracting officer (CO) or contracting officer representative (COR) training
- Compliance with existing regulations
- Size of contracting department as a percentage of personnel in the agency
- Oversight
- Decentralization of contracting processes and management

Play 1 - How Exposed Are You?

Non-financial programs

- Amount of external information to be verified
- Impact on national security or other non-financial area
- History of applicant or party of concern
- Turnover of key staff
- Clearly documented processes and procedures for adjudication
- Source of information
- Type of information (official records versus personal letters)
- Impact of program on other agency operations or programs

Checklist

- ☐ **Identify** the major fraud risk factors in the primary missions of your agency. Use existing documentation, knowledge, IG or GAO audits, or interviews to gather this information.
- ☐ **Determine** the weight of those factors relative to each other based on which are of greatest concern.
- ☐ **Quantify** the risk factors by determining the level to which they expose the program to fraud.
- ☐ **Use** this exercise to focus your efforts on those programs and areas that are most susceptible to fraud.

Play 2 - Know Where You Are and Where You Want to Be

Why is this important

Grading yourself on the maturity of your overall antifraud integrity initiatives can help identify where things are—the current state—and where you want things to be—the goal state. We have identified four stages of a robust antifraud program, ad hoc, initial, operational, and leadership, which are described in the section below.

The Antifraud Program Maturity Model

Are you unsure what level of maturity your agency is currently or where you should be headed? We have developed an example of what the different levels of maturity might look like related to your antifraud initiatives, titled 'The Antifraud Program Maturity Model'. This Maturity Model is a tool to help you self-assess the current antifraud efforts at your agency.

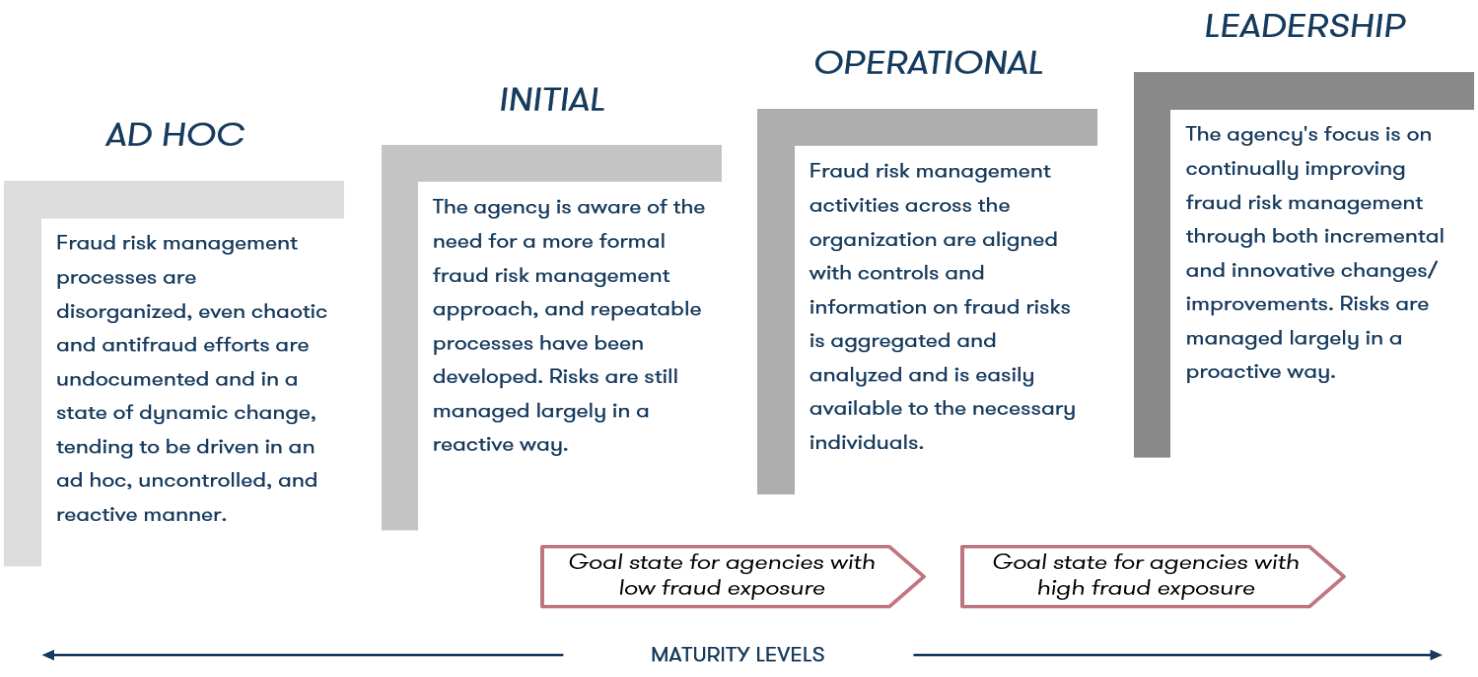


Figure 4: Maturity Model Overview

Play 2 - Know Where You Are and Where You Want to Be

Using this tool, you can effectively conduct a self-assessment and identify the current state and the goal state. It is important to note that the Maturity Model is intended as a guide. You can tailor this transformation to right-size efforts based on key factors such as the size of your agency and your agency's fraud exposure (see *Play 1*), while also considering any environmental factors that may lead to constraints or obstacles in achieving your goal state, such as limited resources.

See 'Key Points' and the 'Checklist' below for vital details and information to help you use this tool effectively.

Click here for access to a full and printable version of the model.

Key Points

- **No two agencies will have the same path** towards their goal state, and you can tailor the *Antifraud Program Maturity Model* to suit the unique circumstances and strategic goals of your agency's antifraud efforts.
- The **goal state for your agency is primarily dependent on your fraud exposure** (see *Play 1*). For example, agencies with a low fraud exposure need not aim for 'Leadership' level maturity, but can instead aim for 'Operational' as their goal state (see *Figure 4*).
- **You can and should right-size efforts based on key factors such as the size of your agency and environmental factors that could impact the achievement of your goal state, such as limited resources.** For example, smaller agencies may not be able to aim for the 'Leadership' level of maturity, and will more likely name 'Initial' or Operational' levels as a goal state. Agencies with limited resources should tailor their plan to ensure it will be feasible with the resources they will have available as they progress towards their goal state.

It is important to note that your Fraud Exposure should be the first factor you consider when identifying your goal state, but considering other factors such as agency size or available resources may provide further insight and help you select an achievable and applicable goal state for your agency.

Play 2 - Know Where You Are and Where You Want to Be

Checklist

- ☐ **Review** the Antifraud Program Maturity Model.
- ☐ **Tailor** the bullets to fit the unique circumstances and strategic goals of your agency.
- ☐ **Evaluate** your agency's current antifraud efforts.
- ☐ **Identify** your agency's 'goal state' based on your current level of maturity (see the *Antifraud Program Maturity Model*), fraud exposure (see *Play 1*), and other key factors such as agency size (see *'Key Points'*).
- ☐ **Pinpoint** the gaps between your current level of maturity and your goal state.
- ☐ **Recognize** and consider the environmental factors that could impact the achievement of your goal state, such as resources, political or legislative policies.
- ☐ **Develop** a "road map" on how you will reach your goal state, considering the environmental factors identified in the previous step.

Play 3 - Fraud is Not a Four-Letter Word

Why is this important?

Promoting fraud awareness throughout the agency from the top down is vital to a strong antifraud culture. Many program managers don't acknowledge that fraud could occur within their programs because of the perception that it equates to poor processes and controls. This needs to change. Discussing fraud within program teams and across programs is a crucial step towards building a fraud aware culture.

KEY POINTS

- **Identifying fraud is not a bad thing** and is vital to improving integrity within your agency.
- Fraud awareness should be **embedded and communicated throughout the agency,** from leadership down to employees **at all levels.**
- Fraud awareness can be **developed through periodic assessment, training, codes of conduct, and frequent communication** (e.g., town hall meetings, fraud newsletters, articles in existing newsletters, and internal social media campaigns).
- Discussing how fraud may occur **takes away the stigma** and helps agency personnel discuss fraud risks openly and thoughtfully.
- Communication methods should be **tailored to best fit the needs of the agency.**

Play 3 - Fraud is Not a Four-Letter Word

Checklist

- ☐ **Coordinate** with your IG to develop materials to support fraud awareness, such as red flags, checklists, brochures, and posters that describe potential fraud and fraud risks.
- ☐ **Host** a fraud awareness event or activity that occurs periodically and involves all levels of the agency, including participation from the IG. For example, consider the following:
    - The Association of Certified Fraud Examiners (ACFE) hosts Fraud Week (usually in November) as a spearhead for building fraud awareness.
    - Hold fraud-focused events such as a fraud knowledge contest to challenge your coworkers to a game of who knows the most about infamous fraud cases.
- ☐ **Publicize** information on antifraud efforts and successfully resolved cases to raise awareness about program integrity and antifraud efforts outside the program.
- ☐ **Weave** frequent fraud discussions into your daily activities, such as discussing fraud topics during regularly scheduled conference calls or meetings with key stakeholders.

Resource Call-Out

Each year, fraud fighters around the world use International Fraud Awareness Week as an opportunity to come together to raise fraud awareness in their communities. Fraud Week (usually in November) is the perfect time to go a step further and start discussions among peers, coworkers, executives and stakeholders in your agency about how important fraud prevention is to your organization.

Play 4 - Create the Antifraud Dream Team

Why is this important

The ACFE 2018 Report to the Nations found that the existence of a dedicated fraud department, function, or team resulted in a 33 percent reduction in median losses from fraud schemes. The antifraud team plays a crucial role in executing your fraud risk management activities because of its fraud expertise and ability to work across agency silos. The team's primary responsibilities are: assessing fraud risks; coordinating risk management processes and mitigation activities; raising fraud awareness; and training agency staff on antifraud policies and procedures.

KEY POINTS

- **You can't be successful without dedicated people** who focus on fraud.
- Your antifraud team should do the following:
    - **Identify an executive sponsor** that is no more than two levels below the agency's top executive (if possible).
    - Act as the **primary champion** for balancing the competing imperatives: mission delivery and fighting fraud. Proactive fraud risk management can help the agency meet its mission more effectively.
    - **Support operations staff** to help solve specific business processes and technical problems related to antifraud activities.

Play 4 - Create the Antifraud Dream Team

KEY POINTS (continued)

- **Have access to data sharing, privacy, and legal expertise.** The antifraud team should help broker agreements to share data internally and externally. This expertise will be necessary to successfully execute those data-sharing arrangements.

- **Design, coordinate, and oversee** fraud risk management activities across the agency and with agencies that share a coordinated mission.

- Function as **a single point of accountability** across the agency, assuming responsibility of addressing fraud and integrating with the myriad of antifraud and other program integrity activities.

- **Coordinate with your IG to provide antifraud training** to agency staff (see *Play 10*) and assist with other fraud-awareness activities (see *Play 3*). Make training CPE eligible to encourage attendance.

- Lead efforts to **take action against identified potential incidents of fraud** (see *Play 15*).

You don't need a large antifraud team to make an impact. *One or two devoted staff is sufficient if they are motivated. A small team can take advantage of resources embedded in program offices to expand their reach and capabilities.*

If your agency has the resources to create a bigger antifraud team, include individuals with ***a mix of operations and fraud expertise based on the types of fraud your agency is most susceptible to*** *(e.g., fraud experts, Certified Fraud Examiners (CFE), grants experts, financial analysts, health clinicians, data scientists). Also, include an IG representative as an ex officio member.*

Your antifraud team should **ACCT**

(Assess, Coordinate, Communicate, and Train).

Play 4 - Create the Antifraud Dream Team

Checklist

- ☐ **Establish** an antifraud team comprised of the right individuals to execute the agency's antifraud strategy, using the guidance outlined in *'Key Points'*.
- ☐ **Develop** clearly defined antifraud team roles and responsibilities.
    - **Coordinate** roles and responsibilities with the agency IG's office, which handles investigations (see *Play 14*).
- ☐ **Assess** fraud risks across the organization (see *Play 6*) by overseeing the fraud risk assessment process.
- ☐ **Coordinate** across business units to streamline risk management activities (e.g., internal controls, improper payments prevention, enterprise risk management) and develop fraud risk responses and mitigation activities.
- ☐ **Communicate** to raise fraud awareness across your agency and establish relationships with program offices.
- ☐ **Train**—develop and deliver antifraud training and fraud-awareness campaigns by leveraging the guidance provided in *Play 3* and *Play 10*. Frequent training can help address the challenge of dealing with evolving, sophisticated fraud schemes.

Identify and Assess

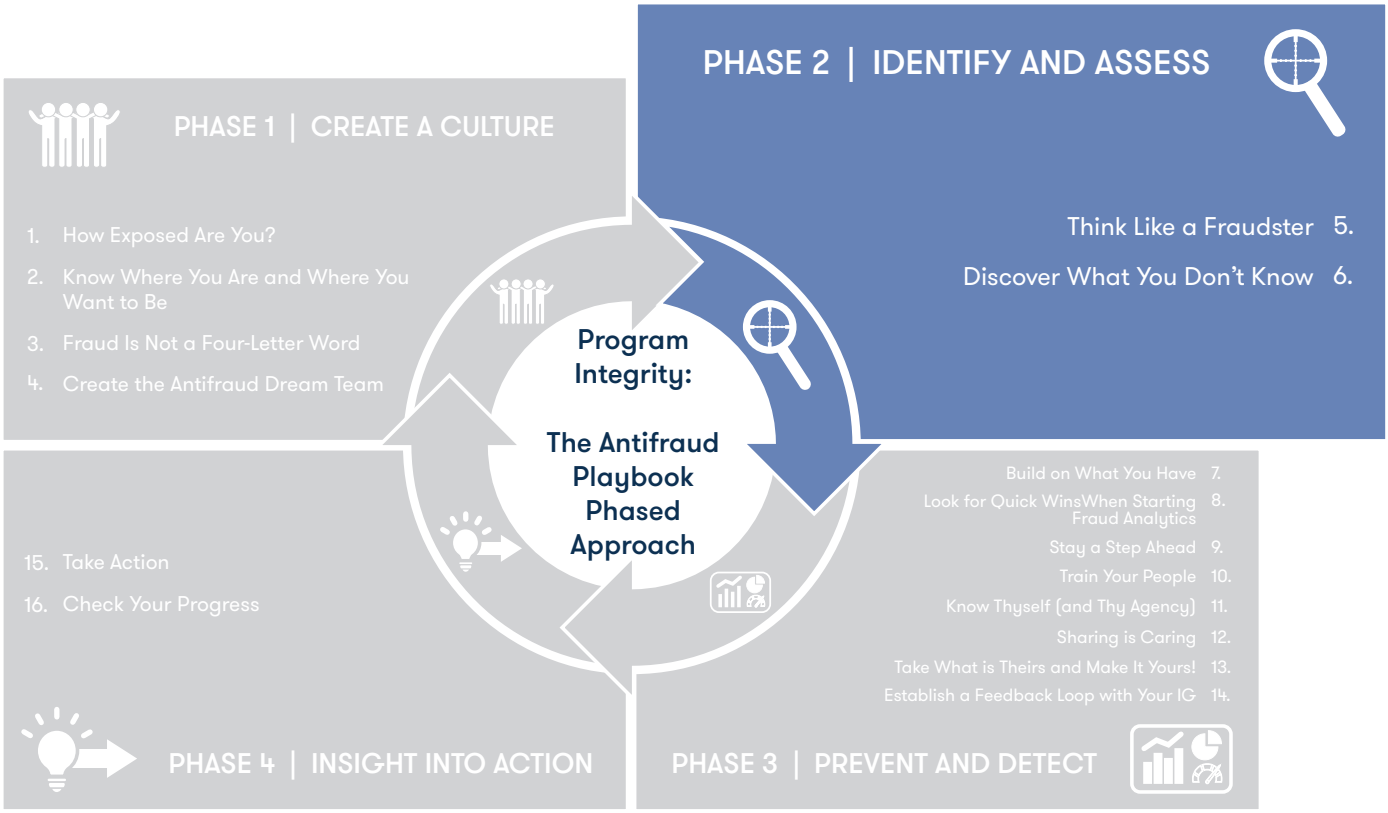


Figure 5: Four-Phased Approach, Identify and Assess

Why is this important

The second phase in the antifraud journey focuses on identifying your fraud risks. A fraud risk assessment is an invaluable tool you can use to uncover your agency's vulnerabilities to fraud. The two plays included within this phase will help you identify your fraud risks and develop a plan for executing a repeatable fraud risk assessment tailored to your agency that you can continue to expand as efforts grow. Note that these plays were designed to align to the leading practices for fraud risk assessment outlined in GAO's Fraud Risk Framework.

What plays are included

5. Think like a Fraudster
6. Discover What You Don't Know

Play 5 - Think Like a Fraudster

Why is this important

Understanding the types of fraud that your agency is vulnerable to, both internal and external, is imperative to developing the right antifraud activities. "Thinking like a fraudster" and coming up with the *fraud schemes* that could be used to commit fraud at your agency is a vital step.

Key Points

- **The best way to begin identifying and understanding your agency's vulnerabilities to fraud is to develop fraud schemes** - scenarios focused on specific programs or processes that highlight potential entry points for fraudulent activities.
- **Fraud can be committed either internally** by employees, managers, officers, or stakeholders of an agency, **or externally** by customers, vendors, and other parties.
- **Not all fraud is financial.** Some fraud can affect an agency's reputation or national security even if it doesn't lead to major financial loss for your agency.
- **The type of fraud you are susceptible to depends on a number of factors.**

For example, there are different fraud risks depending on who makes up your program recipient or beneficiary population, such as Social Security and welfare fraud, Medicare/Medicaid fraud, grant fraud, etc.

For example, fraud tends to flourish when management controls are weak regardless of the specific composition of your target recipient or beneficiary populations.

Play 5 - Think Like a Fraudster

Key Points (continued)

- **When identifying fraud schemes, we recommend doing so in a group setting.** Your efforts will benefit from conversations between relevant stakeholders who understand the functional area, business process, or program for which you are brainstorming fraud schemes, more so than from single individuals brainstorming fraud schemes on their own.

  For example, if you begin this process with the Payroll function, you should ensure you include payroll technicians, supervisors, individuals responsible for policies and procedures related to payroll, to ensure you have a wide array of perspectives and voices, which will lead to a more robust fraud risk map.

- **When identifying fraud schemes, consider both the actor** (i.e., the perpetrator) and the **fraud risk entry points** (i.e., the function or process which the actor capitalizes on to carry out the fraud scheme). See the ***Illustration*** below for examples of possible fraud schemes, actors, and fraud risk entry points.
- The Fraud Triangle is a useful model for **explaining the factors that cause individuals** to commit fraud and can be useful when identifying fraud schemes.

  *Note: For further discussion on the Fraud Triangle see the **'Fraud Triangle: Quick Tip!'**.*

- This process will lead to a comprehensive **Fraud Risk Map** for your agency. A Fraud Risk Map is **a resource that outlines identified potential fraud schemes and other related information for each scheme, such as actor and fraud risk entry point, for various areas within your agency** and is a resource you will be able to **employ across your fraud risk management activities.** For an example, see the ***'Fraud Risk Mapping Exercise'*** below.
- **How should you organize your Fraud Risk Map?** Your Fraud Risk Map can be organized however you would like. We recommend organizing it by your preferred unit of analysis to ensure your Fraud Risk Map aligns to your Fraud Risk Assessment (see ***Play 6***).

  For example, you can break it out by program. In this case, you could group programs with similar processes or missions into a 'program area' and then work to develop fraud schemes for each program within your selected program area. Once completed, you could move onto the next identified program area. This will help you target and streamline your efforts for one program area at a time, ensuring you have a manageable place to start and a plan forward.

- We recommend **your Dream Team** (see ***Play 4***) take on the responsibility for coordinating these activities, ensuring **relevant stakeholders** participate and share their expertise in and knowledge of the specific areas being discussed.

Play 5 - Think Like a Fraudster

FRAUD TRIANGLE: QUICK TIP!

What is the Fraud Triangle? Why is it important?
Donald R. Cressey, a well-known criminologist, developed the Fraud Triangle to answer the following question - why does fraud occur?

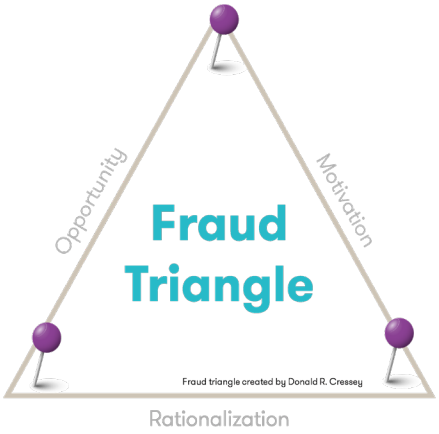


Figure 6: The Fraud Triangle

Cressey's hypothesis was: "Trusted persons become trust violators when they conceive of themselves as having a financial problem which is non-sharable; are aware this problem can be secretly resolved by violation of the position of financial trust; and are able to apply to their own conduct in that situation verbalizations which enable them to adjust their conceptions of themselves as trusted persons with their conceptions of themselves as users of the entrusted funds or property."

The three elements of the Fraud Triangle are: Opportunity, Pressure (also known as incentive or motivation) and Rationalization (sometimes called justification or attitude). For fraud to occur, all three elements must be present.

It is important to understand the Fraud Triangle because **in order to fight fraud effectively you must first acknowledge that fraud occurs and then seek to understand how and why it occurs.** Understanding the Fraud Triangle will provide you with the information you need to understand why fraud occurs.

How can the Fraud Triangle help me?
Understanding the causes that lead someone to partake in fraudulent behavior, i.e., understanding the Fraud Triangle, **can be useful when identifying your fraud risks** and can help you identify more cost-effective means for mitigating your fraud risk.

For example, when it comes to identifying and assessing payroll fraud risks, it can be helpful to assess whether there is a widespread attitude, or rationalization, that everyone lies on their timesheets. If there is, it may be more cost-effective to improve the perception of detection through publicizing detected instances of timesheet fraud than to add additional requirements on managers for verifying the accuracy of time sheets.

Play 5 - Think Like a Fraudster

Checklist

- ☐ **Identify Internal Fraud Schemes.** For example, actors to consider include, but are not limited to:
    - Payroll Staff
    - COs / CORs
    - Management
    - Purchase or Travel Card Holders

    If you have trouble identifying internal fraud schemes, you can consult external and intergovernmental sources for ideas. For example, the ACFE's Fraud Tree outlines the complete classification of internal fraud. You can review the Fraud Tree and identify any internal fraud schemes that your agency might be at risk for, such as theft, misuse of assets, or bribery.

- ☐ **Identify External Fraud Schemes.** For example, you can start this process by identifying the different actors external to your organization that may commit fraud such as:
    - Grantees
    - Medical Providers
    - Beneficiaries (and fraudsters posing as beneficiaries)
    - Contractors

    If you have trouble identifying external fraud schemes, you can consult external and intergovernmental sources for ideas. For example, the Association of Government Accountant's (AGA's) Fraud Prevention Tool outlines resources by business process, program area, and fraud type. Under each option, the AGA outlines risks, fraud schemes, red flags, and best practices/resources. Note: This resource can also be used to identify internal fraud schemes (see the first checklist item).

- ☐ **Develop a Fraud Risk Map.** With the help of research, prior IG and GAO findings, brainstorming, and available external and intergovernmental resources, develop a comprehensive 'Fraud Risk Map', illustrated below, to understand the potential entry points for fraud within your agency.

    Note: The Fraud Risk Map is intended to be a starting point, which will form the foundation of your fraud risk assessment (see Play 6).

Play 5 - Think Like a Fraudster

Fraud Risk Mapping Exercise (Part 1)

The identification of fraud schemes will involve putting on your 'fraudster' cap and walking through possible fraud types (internal and external), fraud risk entry points, and actors to identify vulnerabilities for fraud within individual programs, business processes, and across your agency.

Below we have illustrated an example of a 'Fraud Risk Map' specifically for the payroll function within an agency. This is intended to help you think about where fraud entry points may occur in the payroll function—a thought process you can use at your agency when brainstorming fraud schemes. This illustration focuses on internal fraud, for which we identified three common payroll fraud schemes that a government agency may consider when discussing potential payroll fraud committed by individuals internal to their agency. Remember, this provides some examples to consider, not a comprehensive list of potential fraud schemes within the payroll function.

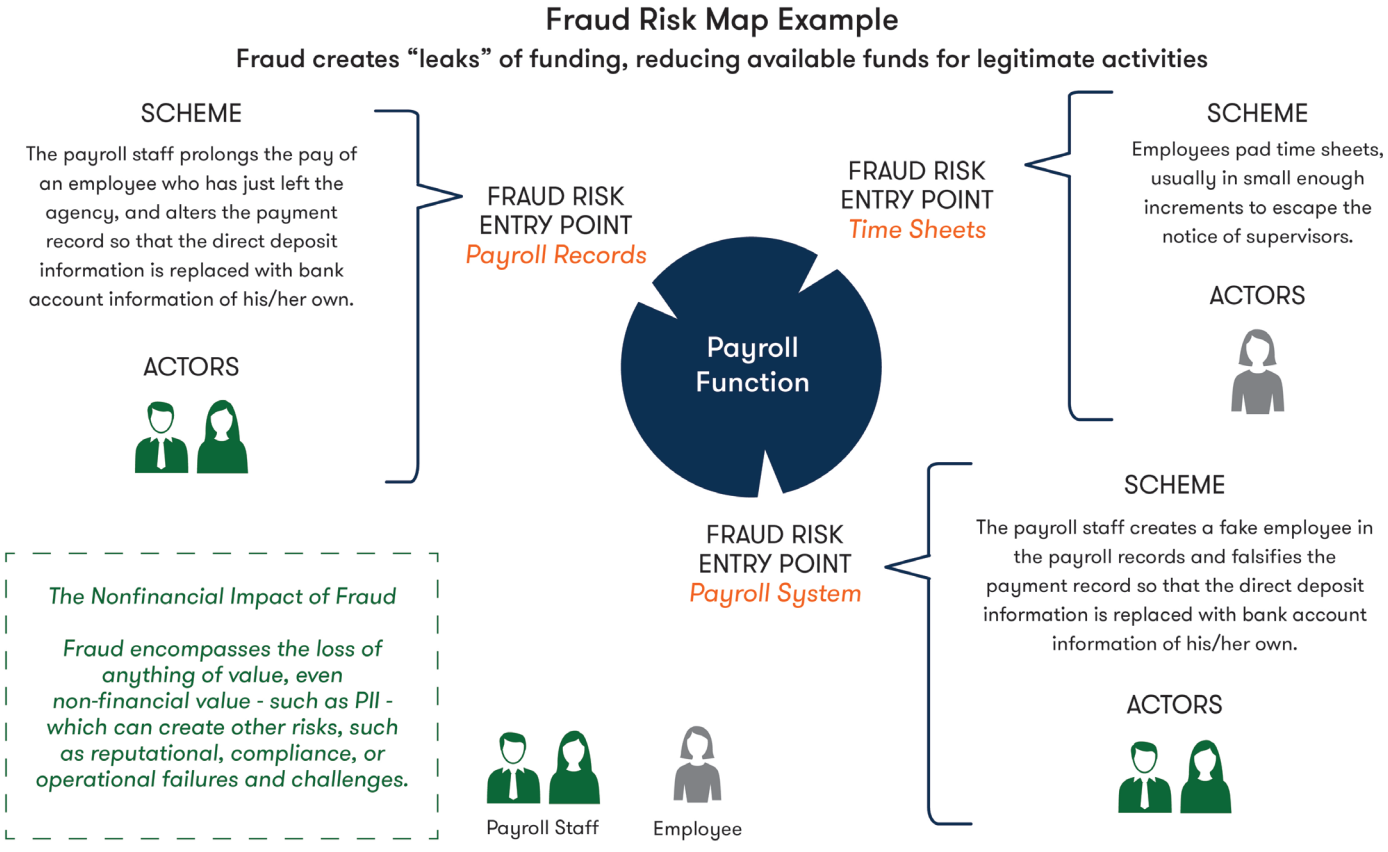


Figure 7: Fraud Risk Map Exercise (Part 1)

Note: The above graphic is included to help you visualize the process for identifying possible fraud schemes, actors, and fraud risk entry points. For a tangible template for how you might record this information, see part 2 of this exercise in Play 7.

Play 6 - Discover What You Don't Know

Why is this important

Fraud risk assessment helps you understand exactly where your processes may be vulnerable to fraud and allows for a holistic look at the fraud risks across the agency. Conducting a fraud risk assessment will shine a light on all the dark corners of your agency's operations and uncover a wealth of previously unknown vulnerabilities to fraud schemes, both internal and external.

KEY POINTS

- The goal of a fraud risk assessment is to **identify and evaluate the potential fraud risks** the agency faces or is most vulnerable to, **analyze the potential likelihood and impact** of fraud schemes identified, and finally to **document and prioritize risks.**

- **The fraud risk assessment process should be visible throughout your agency,** which means you should communicate broadly, promoting the process at all levels of the agency.

- **You do not have to conduct a fraud risk assessment for your entire agency right off the bat.** Starting small and taking an incremental approach to your fraud risk assessment will allow you to learn, iterate, and help you achieve initial successes and gain momentum. This means you can select a starting place that is manageable and expand efforts as resources allow.

- The unit of analysis for your fraud risk assessment is up to you. Generally, **we recommend starting at the component level and then aggregating results to get an agency or enterprise-level view.**

Note: The programs or functions you choose to assess can be defined as any organizational, functional, programmatic or other applicable subdivision of an organization that allows for adequate analysis.

Play 6 - Discover What You Don't Know

KEY POINTS (continued)

- **Consider potential approaches** for selecting a starting point for implementing your fraud risk assessment based on your preferred unit of analysis and the strategic goals, priorities, and the fraud exposure (see *Play 1*) of your agency. Potential approaches include:
    - **Consult the program or function areas your agency uses for other assessments,** such as internal controls testing. These so-called "assessable units" are already established and have a wealth of information that can be used to better inform the fraud risk assessment process.
    - **Assess by program** using a prioritized list of programs based on the fraud risks the programs face. *(Note: the fraud exposure analysis discussed in Play 1 can help develop this list.)* The prioritized list can be translated into a plan for your fraud risk assessment, starting with one or a small handful of programs.
    - **Start with common, data-rich functions,** such as purchase card or travel card programs or payroll systems. Starting with discrete financial management functions has the benefit of being more targeted as potential fraud risks are limited.
- No matter the approach or starting point you choose, **once you have completed the first fraud risk assessments, you will have a repeatable methodology and tangible end-products, such as tools and templates.** Your response strategy can then be enhanced and replicated as you expand the assessment.
- **Fraud risk assessment is more art than science.** There's no one "right way" to assess your fraud risks. Develop an approach and use techniques that work for your agency's culture and fraud exposure.
- **Fraud risk assessment techniques vary,** and you can choose the technique or techniques that best suit your agency. Keep in mind that **not all risk assessment techniques are made equal and you should evaluate the pros and cons of each based on the desired outcomes and circumstances at your agency.** Additionally, keep the risk assessment criteria and responses consistent, even across various techniques, so you can compare the results across the agency. Qualitative risk assessment techniques include but are not limited to:
    - **Focus Groups/Workshops** are the "gold standard" for assessing fraud risks. They involve convening knowledgeable stakeholders in workshops or focus groups. Ideally, these are cross-functional workshops, as they facilitate consideration of risk interactions and break down silos. Workshops can be extremely useful in getting people to have meaningful discussion about how processes and risks interrelate.

Play 6 - Discover What You Don't Know

KEY POINTS (continued)

- **Fraud Scenario Analysis** is a process of analyzing possible future events by considering alternative possible outcomes (sometimes called "alternative worlds"). Thus, scenario analysis, which is one of the main forms of projection, does not try to show one exact picture of the future. It entails identifying fraud risk scenarios, detailing the key assumptions that determine the potential severity of and impact on a key objective. These scenarios can be discussed in cross-functional fraud risk workshops.
- **Surveys** can be useful to gauge items such as the antifraud environment, as they solicit the perspectives of staff across the agency. They can also be useful for large, complex, and geographically distributed enterprises. In general, these surveys should be distributed via an automated online tool or mechanism so that results can easily be consolidated and reviewed.

Note: Surveys should not substitute for workshops and other techniques as drawbacks include:

- *low response rates*
- *difficult to identify information gaps if anonymous*
- *low quality of responses due to time constraints or misunderstanding due to lack of context*
- *no cross-function discussions*

- **Fraud risk assessments should be conducted periodically and when there are changes that could impact fraud risk levels at the agency.** For example, changes to individual programs or the agency's environment could impact fraud risk levels and would lead to a need to re-conduct a fraud risk assessment.

- We recommend your Dream Team (see *Play 4*) take on the responsibility for coordinating these activities. However, the relevant stakeholders from the assessable unit will play a key role as well, such as providing information or developing and owning mitigation activities. **There should be collaboration between the two groups on these efforts, and the exact roles will vary from agency to agency and from one fraud risk assessment to the next.**

- **Consult resources,** such as the AGA Fraud Prevention Toolkit, which contains a Risk Modeling and Assessment page and the GAO Fraud Risk Framework **for additional guidance or materials to further your understanding of the Fraud Risk Assessment process and how it can be tailored to your agency.**

Play 6 - Discover What You Don't Know

Checklist

- ☐ **Identify** the following:
  - Your preferred approach or unit of analysis (see *'Key Points'*).
  - Your starting point within your unit of analysis, i.e., the specific program(s) or function(s) you plan to assess first.
- ☐ **Use** your Fraud Risk Map (see *Play 5*) to identify the types of internal and external fraud risks your chosen starting point faces.
- ☐ **Identify** your preferred risk assessment technique or techniques (see *'Key Points'*) and
  - **gather** information on the controls and processes in place;
  - **determine** if and how the controls and processes in place could be exploited or circumvented; and
  - **assess** the *likelihood and impact* of given schemes being successful.

Keep in mind that using more than one technique will yield better results, since each technique comes with its own benefits and may provide different types of information. For example, you can design and administer a survey that gauges perceptions about the strength of the antifraud culture of your agency, which can be helpful to understand where management and staff may have different views of the culture. You can also conduct focus groups with stakeholders to discuss the controls and processes in place related to the fraud schemes identified, the strength of those controls, and the potential likelihood and impact of the schemes. These will provide different lenses through which you can view your fraud risks.

Note: When assessing likelihood and impact, the specific methodology you choose to use is up to you and will vary based on differences in missions, activities, resources, expertise, and/or other factors. For further discussion on this topic, reference pages 14-15 of GAO's Fraud Risk Framework.

- ☐ **Document** the results of your risk assessment. This includes documenting items such as the likelihood and impact score, the existing controls, or any identified gaps. For example, you can document final likelihood and impact scores for given fraud schemes in addition to any identified controls gaps in your Fraud Risk Map. See the *'Fraud Risk Mapping Exercise (Part 2)'* for an example of how you can document this information.
- ☐ **Translate** the fraud schemes into specific risks. For example, if the fraud scheme you were discussing related to a contractor overbilling for services, the specific risks you may identify include:
  - Contractors bill for goods or services that were not provided, which results in financial loss to the agency.
  - Contractors overbill for goods or services that were provided, which results in financial loss to the agency.

These specific risks should align to the fraud schemes assessed, but call out the specific risk associated with the scheme. In the examples above, the risk we identified was financial loss, but it can be anything you may discuss or identify in your assessment as a potential risk to your agency of the particular fraud scheme.

Play 6 - Discover What You Don't Know

Checklist (continued)

- □ **Determine** your fraud risk tolerance (see the *'Fraud Risk Tolerance: Quick Tip!'* for further details).

- □ **Prioritize** risks based on the results of the assessment and your fraud risk tolerance. For example, you can prioritize risks based on likelihood and impact scores or strategic priorities. No matter how you decide to prioritize risks, ensure that you consider the extent to which control activities currently in place mitigate the likelihood and impact of risks and whether the remaining risk after considering those control activities exceed your fraud risk tolerance.

- □ **Develop** responses to mitigate the likelihood and impact of risks, including the identification of "owners" for each response activity. Responding to fraud risks is imperative to successful and effective fraud risk management.

When responding to risks, you have a few options as defined in the Green Book:

- ***Accept*** *- No action is taken to respond to the risk based on the insignificance of the risk.*
- ***Avoid*** *- Action is taken to stop the operational process or the part of the operational process causing the risk.*
- ***Reduce*** *- Action is taken to reduce the likelihood or magnitude of the risk.*
- ***Share*** *- Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.*

You may find a particular type of risk requires the following:

- ***Combination Approach****—A particular risk may require more than one response activity to address certain aspects of the risk, such as accepting part of the risk and reducing another element of the risk through the implementation of additional control activities.*

It is important to note that if you choose to "accept" a risk, there will be no mitigating actions developed. For example, you may decide to allocate resources to mitigate fraud risks identified that exceed your fraud risk tolerance level. However, for fraud risks that were determined to be unlikely or low-impact or for risks that fall within your fraud risk tolerance level, you may decide to "accept" these fraud risks and take no further action. Be sure to document your process and rationale for taking no action.

However, if you choose one of the other response activities, you will have to design and implement specific mitigation and/or control activities to respond to the specific fraud risks, which will in turn assist in the prevention and detection fraud at your agency.

Play 6 - Discover What You Don't Know

Checklist (continued)

- ☐ **Document** the fraud risk profile. Called for in GAO's Fraud Risk Framework, a fraud risk profile is essentially a summary of the outputs of the fraud risk assessment process and should at a minimum include the high priority fraud schemes, likelihood and impact, risk tolerance, risk prioritization, response activity, and owner.

  You should develop a separate fraud risk profile for each unit of analysis (see 'Key Points'). For example, if your unit of analysis is at the program level then each program would have a tailored fraud risk profile upon completion of its fraud risk assessment. This could then be rolled-up to the agency level to gain an enterprise-wide view.

- ☐ **Report** the results. The results of your fraud risk assessment should be summarized and reported to relevant agency stakeholders. Note that sharing information about your fraud risk tolerance outside the agency or outside senior leadership within the agency is not necessary and may not be advisable. Hesitance to share this information should not be cause for failing to conduct the analysis.
- ☐ **Evaluate** the effectiveness of your risk assessment and make changes to the process based on lessons learned, successes, and pitfalls.
- ☐ **Repeat and update** this process for the selected assessable unit iteratively as you learn and as your efforts mature. A fraud risk assessment is not a "one-and-done" activity, you will have to periodically re-conduct the fraud risk assessment for each assessable unit.
- ☐ **Expand** the risk assessment to other areas, or assessable units, based on your preferred approach.
- ☐ **Aggregate** results for each assessable unit in which you conduct a risk assessment to develop an agency level view of your fraud risk and identify trends.

Figure 8 shows at a high level how this checklist aligns to GAO's Fraud Risk Framework.

See Appendix A for a more detailed graphic.

Play 6 - Discover What You Don't Know

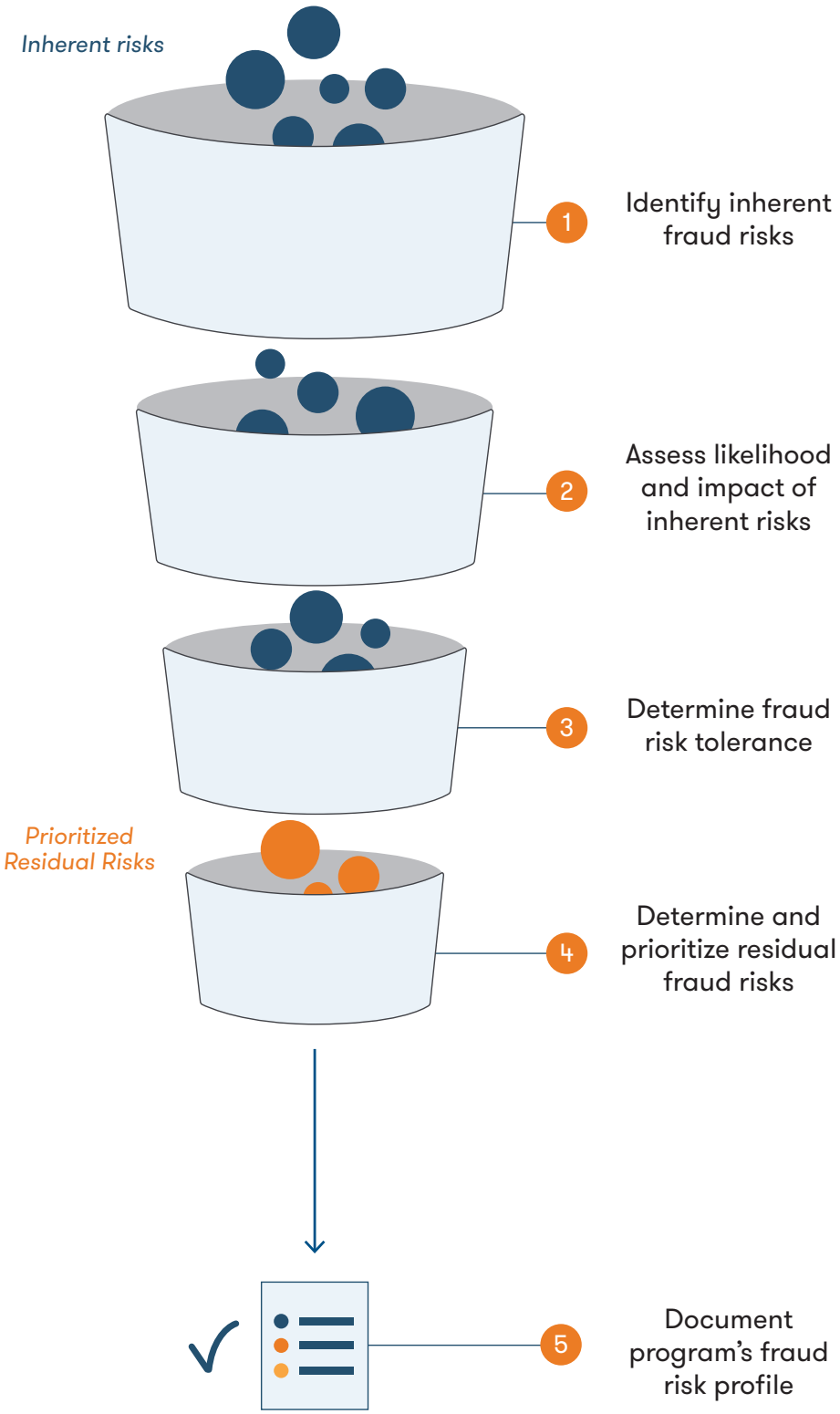


Figure 8: The Five Phases of the GAO Fraud Risk Framework

Play 6 - Discover What You Don't Know

FRAUD RISK TOLERANCE: QUICK TIP!

What is Fraud Risk Tolerance?
According to the Green Book, risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. How does this translate to fraud? Your fraud risk tolerance reflects the thresholds related to fraud risk above which you feel it is necessary, from a cost or reputational standpoint, to mitigate. In other words, **your fraud risk tolerance expresses your agency's willingness to tolerate an estimated amount of fraudulent activity. [Note: Zero tolerance may be the right answer from a public relations perspective, but it's unrealistic in practice.]**

Your risk tolerance may depend on factors such as the individual circumstances of a program, the cost-benefit of implementing activities to reduce the risk of fraud, resource or other constraints, reputational risk, etc.

Defining your Level of Tolerable Risk
You can express your fraud risk tolerance quantitatively or qualitatively, and no matter which method you choose your tolerance level should be **specific and measurable.** For an example and further discussion related to this topic, reference pages 13 - 15 of GAO's Fraud Risk Framework.

Play 6 - Discover What You Don't Know

Fraud Risk Mapping Exercise (Part 2)

Risk Assessment techniques may vary, but in order to be effective you must have a comprehensive view of the fraud risks your agencies face. **Using the Fraud Risk Map you have developed** (see *Play 5*), you can now **build out additional information** to help facilitate the risk assessment process and upon completion of the fraud risk assessment process.

In the table below, we built out items for identified fraud schemes, such as fraud type, fraud risk entry point, actor, likelihood, impact, and risk score (see the fourth checkbox item in the *'Checklist'*). It is important to note that **this can include a number of additional items such as specific risks related to the fraud scheme, internal controls gaps identified, response strategy, and owner** based on the information you gather as part of the assessment process and how you plan to move forward with the collected information.

Program Name	Fraud Category	Fraud Risk Entry Point	Actor	*Fraud Scheme*	Likelihood	Impact	Risk Score (Likelihood x Impact)
Payroll	Ghost Employee	Payroll System	Payroll Staff	*The payroll staff creates a fake employee in the payroll records and falsifies the payment record so that the direct deposit information is replaced with bank account information of his/her own.*	**3**	**3**	9
Payroll	Unauthorized Hours	Timesheet	Employee	*Employees pad time sheets, usually in small enough increments to escape the notice of supervisors.*	**5**	**3**	20
Payroll	Ghost Employee	Payroll Records	Payroll Staff	*The payroll staff prolongs the pay of an employee who has just left the agency, and alters the payment record so that the direct deposit information is replaced with bank account information of his/her own.*	**3**	**4**	12

Table 3: Fraud Risk Map Exercise (Part 2)

Play 6 - Discover What You Don't Know

Fraud Risk Mapping Exercise (Part 2)

In **Table 3**, we expanded our Fraud Risk map to include the results of the fraud risk assessment process. In our example, we only included likelihood, impact, and risk score, but the intention is to show how you can transform your Fraud Risk Map into a tailored Fraud Risk Profile (see the *'Checklist'*). As a reminder, a Fraud Risk Profile is essentially a summary of the outputs of the fraud risk assessment process and should at a minimum include the high priority fraud schemes, likelihood and impact, risk tolerance, risk prioritization, response activity, and owner. You can use Table 3 as a guide and build out the additional information recommended to develop your own Fraud Risk Profile. See the attachments at the left-hand side of this PDF to view an Excel version of the above table.

Note: The likelihood and impact scores provided in the table above are illustrative. They do not reflect the actual likelihood and impact of these proposed schemes, as this would differ from agency to agency. Additionally, 'Risk Score' was calculated by multiplying likelihood by impact using a 1-5 likelihood and impact scale. See the ***'Fraud Risk Scoring Handout'*** *for further details on fraud risk scoring.*

Note: This listing of fraud entry point questions is not intended to be all inclusive, but you can use it as a starting point for discussion or to brainstorm your won fraud entry point questions.

Prevent and Detect

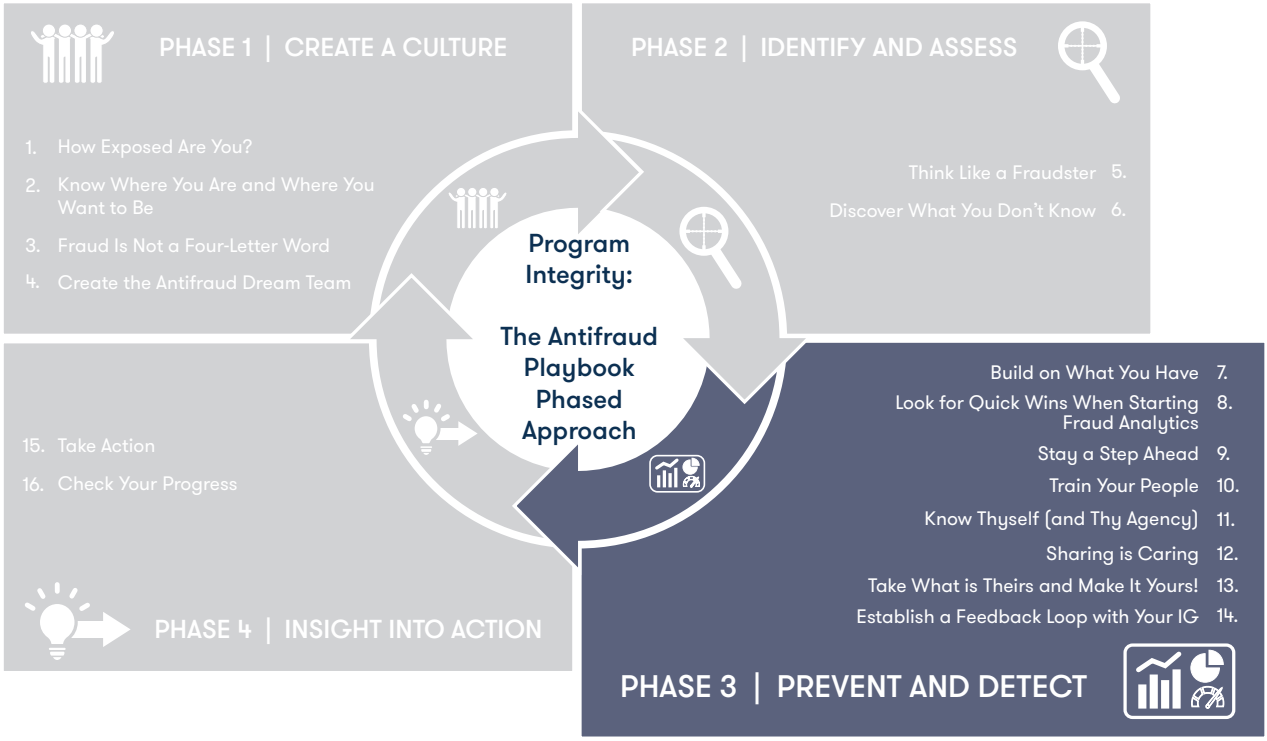


Figure 9: Four-Phased Approach, Prevent and Detect

Why is this important

The third phase in your antifraud journey is about putting in place or strengthening fraud-centric controls to mitigate the risks you identified in the previous phase (see the *'Identify and Assess'* page).

In this phase, we provide actionable guidance on a number of items. This phase includes plays related to leveraging existing risk management activities (see *Play 7*) and designing and implementing specific control activities such as data analytics (see *Play 8* and *Play 9*) and targeted antifraud trainings (see *Play 10*). This phase also includes plays that focus on establishing collaborative relationships both internally and externally to share information and lessons learned (see *Play 11*, *Play 12*, *Play 13*, and *Play 14*).

The eight plays included within this phase will help you use your current risk management efforts, design and implement specific control activities, and collaborate with relevant parties to share information and capitalize on it.

What plays are included

7. Build on What You Have
8. Look for Quick Wins When Starting Fraud Analytics
9. Stay a Step Ahead
10. Train Your People
11. Know Thyself (and Thy Agency)
12. Sharing Is Caring
13. Take What is Theirs and Make It Yours!
14. Establish a Feedback Loop with Your IG

Play 7 - Build on What You Have

Why is this important

Most agencies have developed enterprise risk management (ERM) functions and have mature financial reporting, improper payments, and internal control programs. Building on these existing efforts will keep you from reinventing the wheel. This will not only be more effective but will likely increase adoption and support from those already working in these areas.

KEY POINTS

- **Draw on the lessons learned from other reporting and risk management efforts** such as your ERM program, improper payment process, internal controls program, or reports from the IG and GAO.
- **Use templates, processes, tools, and existing data** from other efforts and expand on those. Build on existing fraud related efforts if they exist. Don't start from scratch—modify and use what is already being done. Conversely, consider how what you do create can be used by other efforts.
- **Consider financial and non-financial efforts** in order to incorporate all practices in your organization.
- **Seek out feedback** from program managers who have in depth knowledge of other efforts in your agency.

Play 7 - Build on What You Have

Checklist

- ☐ **Solicit** input from program managers and leadership on what kind of fraud efforts would be most useful to them.
- ☐ **Identify** other efforts you could learn from or expand upon, and coordinate with the leaders of those efforts to consolidate them. These leaders may also have insights to consider as you move forward.
- ☐ **Create** a communication strategy that conveys these consolidation efforts throughout your agency. Work with the antifraud team in this and other efforts (see *Play 4*).

Illustration

If you have already implemented an ERM program, you can use the risk profile templates, data collection processes, and scoring methodologies as part of your fraud risk management efforts. Using similar templates for ERM and fraud risk management efforts will help you present new information in a familiar format. Further, consolidating your data collection processes can help you obtain information in an efficient manner that minimizes the burden in your program or agency. Conversely, if you have a new idea or initiative that will help in fraud risk management, socializing it with ERM or other efforts may yield ways to use that idea across the agency. For example, fraud risk assessment work at the Veteran's Administration incorporated IPERA work after the agency found it more efficient to combine the two. In order to make the most of your efforts, your agency should coordinate your fraud risk management program, ERM program, and IT efforts. When in concert, these efforts can reinforce each other as fraud risk management will play a role in ERM, and IT efforts will be part of the data management and analytics that you may use in fraud risk management and ERM programs.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

Why is this important

The ACFE 2018 Report to the Nations found that organizations **using data analytics techniques to fight fraud reduced the cost of fraud schemes by 52 percent and reduced the duration by 58 percent.** The most effective antifraud control you can put in place is a data analytics tool of some sort, which doesn't have to be costly and complex—it can be a low-tech, open-sourced software that identifies suspicious transactions or behaviors.

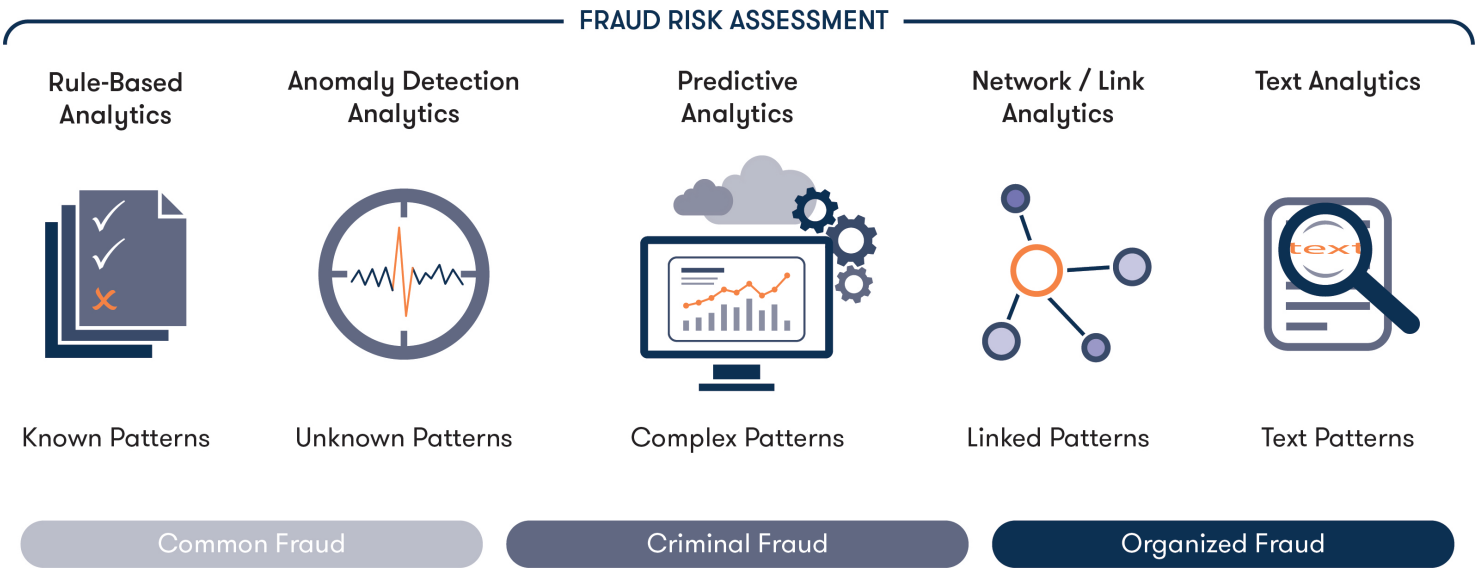


Figure 10: Fraud Risk Analytics Overview

There are a lot of analytics techniques out there. In the graphic above, we outline five different techniques ranging from simple to more advanced. Below, we provide a description of each technique:

Play 8 - Look for Quick Wins When Starting Fraud Analytics

- **Rule-based**—A transaction level technique to prevent common fraud based on known patterns. Rule based analytics focuses on transactional data which does not adhere to organizationally accepted rules, such as using a purchase card on a Saturday evening or federal holiday.
- **Anomaly detection**—Focused on investigating aggregate-level transactions, anomaly detection uses "unsupervised modeling" to identify outliers compared to peer groups based on unknown patterns among common and individual fraudsters. This type of analytics technique allows organizations to understand outlier patterns across the data that may suggest fraud and flag for investigation.
- **Predictive Analytics**—As patterns become more complex and criminal fraud manifests into organized fraud, predictive analytics can identify unobserved attributes that lead to suspicion of fraud based on known cases of fraud. For example, the analytics model could automatically reject a payment when the existence of a number of known fraudulent characteristics is present. Predictive analytics generally uses machine learning techniques to stop payments, rather than flagging transactions for investigation.
- **Network/Link Analytics**—This technique can be useful for uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery. For example, an individual may not be suspicious based on their actions alone, yet suspicion may arise when their actions are connected to others through a set of commonalities based on associated attributes, revealing schemes that may have otherwise gone unnoticed.
- **Text Analytics:** A technique that involves scraping the internet of things (IoT) information into a structured form and parsing strings of text to scan for red flags of fraud. The parsing occurs by using natural language processing (NLG) tools that divide the body of text into segments which are analyzed for text patterns and then described in terms of their syntactic roles, resulting in a sentiment or polarity analysis.

In this play, we will be focused on the more simple techniques, such as rule-based analytics, which may provide quick wins based on high-impact and low-effort to develop. For a discussion on more evolved techniques, such as text analytics, see *Play 9*.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

KEY POINTS

- Data analytics, as it applies to fraud, refers to the use of analytics to **identify trends, patterns, anomalies, and exceptions within data** to identify indicators of fraud.

- **Fraud impacts every agency** in various ways and while the factors that contribute to fraud differ from agency to agency, the process by which schemes can be identified follows similar steps. Sharing tools, techniques, and best practices can be very effective.

- ***You don't have to do it alone.*** If you don't have analytics capabilities in-house you can consult government-wide resources, such as the Do Not Pay Business Center. Also consider asking contractors to walk you through the process step by step.

- **Do the best you can with the data you have.** Not having the "right" data or "clean" data is often used as a roadblock for implementing fraud-specific analytics. However, you would be surprised with what you can do with the data you have available, so don't let that stop you from starting your analytics journey.

- **Relevant data can come from numerous sources** and take on many forms, including accounting and financial data, vendor data, or even internal communications and documents. Remember, not all fraud is financial so not all data must be financial to be relevant.

- **Consider potential approaches** for selecting a starting point for implementing analytics. Potential approaches include:
    - **Targeting common fraud scenarios** that all agencies face (see *Play 5*), such as purchase card and payroll fraud as a starting point for your initial analytics efforts. Note that many credit card companies will offer agencies fraud analytics tools free of charge.
    - **Focus on high risk areas** identified through your fraud risk assessment (see *Play 6*).

- **Consider known or previously encountered fraud schemes to design your analytics tests.** If you consult information related to previously encountered fraud or known fraud risks identified through your fraud risk assessment (*Play 6*), you can identify red flags of fraud that may exist in your data. Many fraudsters find success in copying known schemes across the industry, so running tests for these schemes is an excellent place to start with analytics.

For example, if your agency has rules in place that prohibit purchase card transactions on a federal holiday, then testing your transaction data to identify purchases from cardholders that fall on federal holidays may help you identify suspicious transactions.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

KEY POINTS (continued)

- **It is simpler to identify the data you need once you have a starting point in mind.** For example, if you plan to use high risk areas identified through your fraud risk assessment (*Play 7*) as your starting point for analytics, you will have a clear idea of the type of data and tests required to implement successful analytics solutions specific to that high risk area.

- **Combine data across programs and from separate databases** within the agency and outside the agency to facilitate and inform reporting and analytics when possible (see *Play 11*, *Play 12*, *Play 13*, and *Play 14*). We know this may be easier said than done, so when in doubt use the data that is available to you within your agency and integrate additional data sources as feasible as you mature your analytics.

- **Consult your agency's Office of Inspector General (OIG)** when possible in this process. Some OIG's are heavily involved in data analytics and may be able to assist in this process or provide data or information that you can use. See *Play 14* for further details on how to integrate with your OIG.

- Understand that **the process is iterative**, and should adapt as your data analytics efforts mature. Focus on quick wins when first setting up the analytics solutions and become more complex once you are ready. Attempting complex analytics solutions too quickly may decrease your team's adoption rate or use of analytics for future fraud initiatives.

- **Design a data analytics strategy/process** that clearly identifies and fully explains:

    - What organizational data is available and accessible
    - When and how to obtain the organizational data
    - How to integrate the process into the organization's fraud risk assessment program
    - What data analytics tools and techniques to use for evaluating the potential existence of fraud
    - What data analytics talent is available in-house between federal employees and contractors
    - What data analytics services are available at other agencies that could enhance your efforts
    - What governance needs to be put in place so the solution is sustainable
    - How to evaluate the process's effectiveness in detecting and preventing fraud
    - How to clearly communicate findings and report recommendations

Play 8 - Look for Quick Wins When Starting Fraud Analytics

Checklist

- ☐ **Identify** your starting point (see *'Key Points'*).
- ☐ **Identify** all available data associated with your starting point. For example, if you are targeting purchasing or procurement fraud, you may focus on available vendor data.
- ☐ **Identify** an analytics model or set of tests that is best suited for your targeted area. Common and more simplistic analytics models to consider include:
    - **Rule-based**—As described above, this is a transaction-level technique to prevent common fraud based on known patterns. Rule-based analytics focuses on transactional data which does not adhere to organizationally accepted rules. This technique results in the identification of departures from expected procedures for additional investigation.

For example, purchase cards cannot be used to purchase alcohol (the "rule") so identifying purchase card transactions for alcohol sales would be a "rule break" and would be flagged.

    - **Anomaly detection**—As described above, this technique focuses on investigating aggregate-level transactions to identify outliers compared to peer groups based on unknown patterns among common and criminal fraudsters. This type of analytics technique can help the agency learn the patterns in the data that may suggest fraud. This will allow you to identify aggregate abnormal patterns that don't conform to established normal behaviors, i.e., outliers.

For example, if a physician is charging for more than 24 hours in a day, this would be flagged as an abnormal billing pattern.

You may also consider common analytics tests as part of this process. For example, if you are targeting purchasing or procurement fraud, you could perform the following analytics test with available data:

- Look for one-time vendors or vendors with expedited payments.
- Compare purchases by ordering clerk for each vendor and product to identify vendor preference patterns.
- Compare employee names, addresses, and account information to vendor master information to identify potential conflicts of interests or hidden relationships.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

Checklist (continued)

- ☐ **Implement** your chosen analytics model(s) and test(s).

  When implementing your chosen analytics model(s) and/or test)s), it is important to note that you can utilize existing, free and low-cost analytics tools if your agency is resource constrained to carry out your model(s) and/or test(s). It is recommended to begin with low-cost software solutions or with a small software purchase prior to making large, enterprise purchases without a known ROI.

  - *For example, Microsoft Excel and Microsoft Power BI are two low-cost options that most agencies already have access to as part of the Microsoft 365 package.*
  - *For example, financial institutions that are federal purchase card providers sometimes offer dashboard capabilities to help agencies identify suspicious purchases.*

- ☐ **Review** the results and refer appropriate cases to the OIG for further investigation.

  This includes reviewing potential incidents of fraud to remove false positives, verify the facts and circumstances, identify similar cases, and checking for math or other errors. See Appendix III of GAO's Fraud Risk Framework for further details.

- ☐ **Identify and report** findings and recommendations based on the results to relevant stakeholders.

  For example, if you have findings and recommendations related to your agency's contract or procurement function, you should not only communicate those to leadership but you should also communicate the results to relevant stakeholders within that function. This will allow that group to incorporate lessons learned and improve fraud risk management activities within their particular function or program, such as updating a policy to include a newly identified internal control to combat a fraud risk identified through analytics.

  Note: We recommend tailoring the report for your intended audience to ensure the results are useable and to ensure their effectiveness. For example, if your intended audience is senior leadership, then presenting your findings and recommendations in a visual manner and focusing on the most important items instead of going into all the specific details may be best. However, if you are presenting to program stakeholders then tailor the results to showcase the items that affect the day-to-day work or items that they have ownership of so that they are aware of their risks and can begin work on mitigating them.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

Checklist (continued)

- ☐ **Evaluate** the effectiveness of your analytics model(s) and test(s) in detecting and preventing fraud.

  *For example, when using simpler analytics techniques such as rule-based analytics, you can evaluate the effectiveness of your model based on identified instances of fraud. If your rule-based model is used to stop payments or transactions, then you can investigate a sample of those to see whether they were indeed fraud and therefore evaluate how well the model performed. You can coordinate with the IG (see **Play 14**) to inform this process.*

  *When using more evolved analytics techniques (see **Play 9**) such as predictive analytics, you may determine your model's accuracy and error rate in predicting cases of fraud during the "training" process. As known cases of fraud are identified, you may improve the characteristics your models use to identify fraud. This is performed optimally by collaborating with the OIG office in feeding known cases of fraud back to the analytics and Program Integrity teams for model refinement. This process is the basis of machine learning.*

- ☐ **Repeat and update** this process iteratively as you learn from your analytics model and tests and as your efforts mature.

- ☐ **Expand** your analytics to other areas, such as other high risk areas identified through your fraud risk assessment and/or by targeting additional common fraud scenarios (see *'Key Points'*).

Play 8 - Look for Quick Wins When Starting Fraud Analytics

FRAUD DATA ANALYTICS: QUICK TIP!

How to Use your Fraud Risk Assessment

The fraud risk assessment process (see *Play 6*) naturally leads to the identification of fraud risks, red flags, and business rules that can be leveraged to develop analytics models and tests.

For example, let's say that during the fraud risk assessment process you identify the following fraud scheme related to your benefit payments -

- A beneficiary claims a dependent that is over 18, which is outside of the allotted range, to increase their benefit payments.

In this example, we will use rule-based analytics. So our first step would be to identify the business rule associated with the fraud scheme and the related "rule-break". This would look something like the following -

- Beneficiaries cannot claim dependents over the age of 18—the "rule"—so identifying dependents over the age of 18 would be a "rule-break" and would be flagged.

Additional examples of fraud schemes translated into business rules and related "rule-breaks" are shown below.

Business Rule	*Rule-Break*
Income tax return must be for a living individual	*Tax return filed with a Social Security Number on the Death Master File*
Health care provider claims must have a valid date of service for a covered service	*Health care provider submits claim for non-covered service pre-dating coverage period*
Agency purchase card transactions are exclusively for business purposes	*Employee charges for personal expenses (gas for a personal vehicle)*

Table 4: Rule-Based Analytics Examples

Play 9 - Stay a Step Ahead

Why is this important

Your analytics capabilities will evolve with your fraud risk management program. Establishing a robust fraud analytics effort will take you from a "pay-and-chase" approach to a predictive approach so you can identify instances of potential fraud before they even occur. Not every agency will maintain in-house analytics capabilities that are continually evolving; for some agencies the size or cost of the program may be too large to effectively implement. In those situations, it is just as important to look outside the agency for opportunities to use shared analytics resources. An evolving approach to fraud risk management will help you stay ahead of the changes in schemes and technology that fraudsters will try to adopt and utilize.

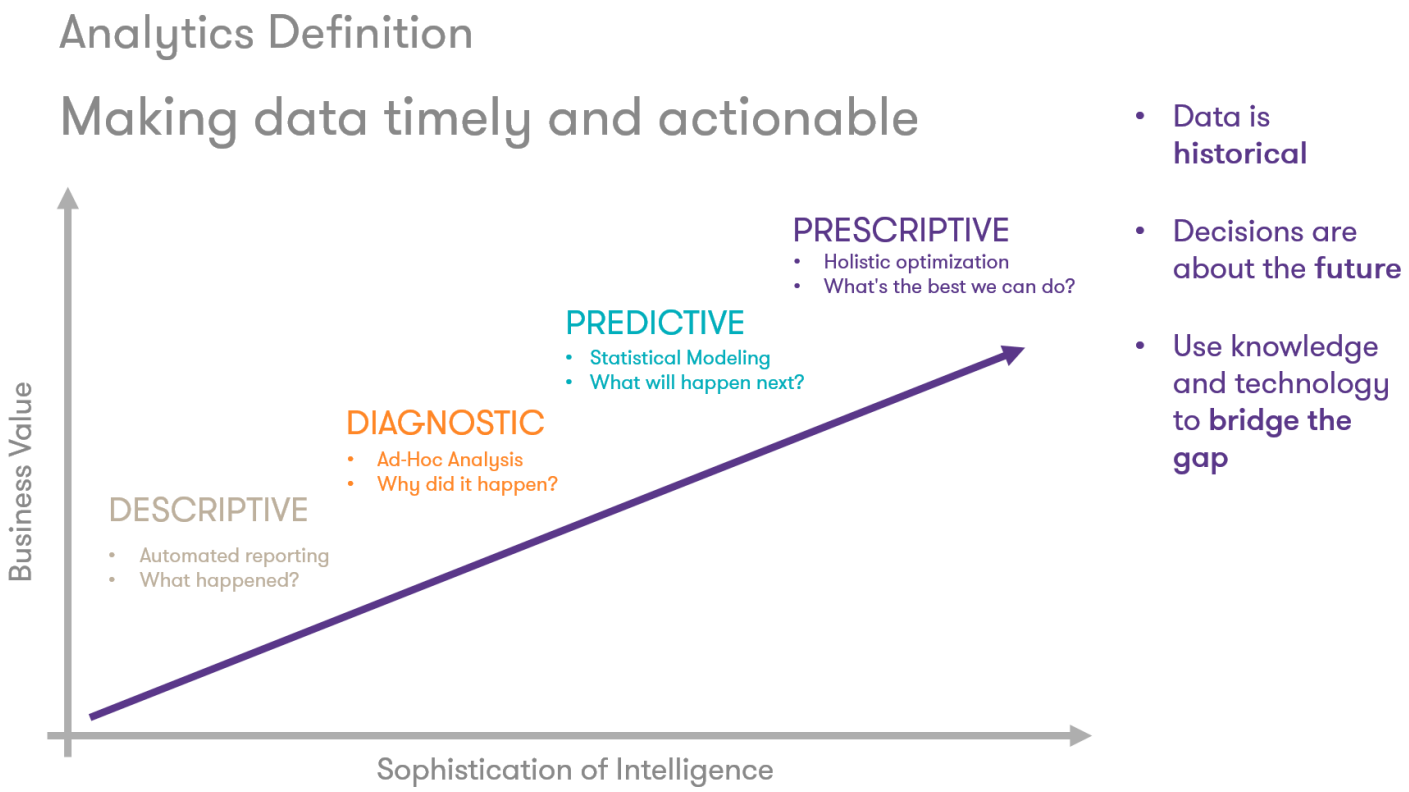


Figure 11: Defining and Evolving Your Analytics Program

Play 9 - Stay a Step Ahead

KEY POINTS

- In evolving your analytics program **continually incorporate business rules based on the experiences of the agency.**
- **Use your experiences looking at external data to build the higher quality data sets** that can help in your analytics program. As you refine the models with better data, you can "train the machine" to know when a certain data point is fraud, which is the basis for predictive, machine learning analytics.
- If you need more advanced analytics capabilities but aren't in a position to build your own program, **check with other agencies who might be able to help or seek out a shared analytics service**. Often times it is more cost effective to use what is already out there than to build something from scratch.
- **More developed analytics programs can predict fraud** by identifying a potential fraud based on the known fraud cases in the model.
- **Evolving your analytics program is not a solo effort**; talk to your colleagues across government and learn what tools and techniques have and haven't worked in more advanced programs.
- **Design a data analytics strategy/process** that clearly identifies and fully explains:
    - Can my data analytics program identify instances of potential fraud and stop fraudulent payments based on tested business rules?
    - Does my data analytics program continually look for business rules to incorporate and higher quality data to utilize?

Checklist

- □ **Use** your early analytics efforts and results (see *Play 8*) to identify a starting point for implementing more advanced analytics capabilities, perhaps focusing on areas of higher risk (see *Play 6*), areas with large volumes of available data, or fraud schemes or patterns that emerged from your early analytics tests.
- □ **Determine** which analytics model(s) is best suited for your targeted area. More evolved analytics models to consider include:

Play 9 - Stay a Step Ahead

Checklist (continued)

- **Predictive Analytics**: As described above in Play 8, this technique can identify unobserved attributes that lead to suspicion of fraud based on known cases of fraud. For example, the analytics model could automatically reject a payment when the existence of a number of known fraudulent characteristics is present. Typically predictive analytics are using machine learning techniques, rather than flagging transactions for follow up investigation.

- **Network / Link Analytics**: As described above in Play 8, this technique can be useful in uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery. For example, an individual may not be suspicious on his or her own, but when submitted to link analysis, his or her known associates could be engaged in well-known fraud schemes which would merit further scrutiny.

- **Text Analytics**: As described above in Play 8, this technique can parse reviews and information for red flags of fraud looking at text patterns.

  *Note: See **Figure 10** in Play 8 for further details on these analytics models.*

□ **Implement** your chosen analytics model(s) and test(s).

□ **Review** the results and refer appropriate cases to the OIG for further investigation.

□ **Identify and report** findings and recommendations based on the results to relevant stakeholders.

□ **Evaluate** the effectiveness of your analytics model(s) and test(s) in detecting and preventing fraud.

□ **Repeat and update** this process iteratively as you learn from your analytics model and tests and as your efforts mature.

□ **Expand** your analytics to other areas, such as other high risk areas identified through your fraud risk assessment and/or by targeting additional common fraud scenarios (see *'Key Points'*).

Play 9 - Stay a Step Ahead

Illustration: Building an Antifraud Analytics Capability Takes Patience

The Centers for Medicare and Medicaid Services (CMS) and the Social Security Administration have predictive capabilities in their analytics programs based on business rules. According to its website, CMS's Center for Program Integrity estimates that the next generation of its Fraud Prevention System will result in a 20 percent savings increase over the already substantial returns of their predictive analytics capabilities. These programs have not occurred overnight or just because there was funding. These two agencies exemplify the patience and thought needed to build such programs and have them succeed. What works for other agencies may not work for yours, and discerning between the two is the key to making sure you don't take a step backward in your program. Predictive analytics capabilities should be built after a program evolves through more standard capabilities that are also more cost effective—a process that both CMS and the Social Security Administration went through to arrive at their current analytics state.

Play 10 - Train Your People

Why is this important

The ACFE 2018 Report to the Nations found that fraud training for employees resulted in a 41 percent reduction in median losses from fraud schemes. Targeted antifraud training developed in coordination with your IG is an incredibly helpful way to help agency employees better identify suspicious activity and feel empowered to take action against potential fraud. Antifraud training raises awareness and is an effective tool to communicate solutions to help prevent fraud, resolve fraud cases more quickly, and more effectively deliver your agency's mission.

According to the ACFE's 2018 Report to the Nations, tips are the most common fraud detection method. Antifraud training should address agency-specific fraud concerns and educate employees and third parties about reporting systems and how to report fraud.

KEY POINTS

- Key elements to consider when developing an antifraud training program:
  - Who should attend;
  - Training frequency and duration;
  - Content and resources;
  - Cultural sensitivities; and
  - Delivery methods that best fit the needs of your organization.
- An effective training program should provide **recurring sessions that address agency-specific fraud concerns** and provide employees **with practical knowledge** and material they can use in their day-to-day work.
- Training should offer **agency-specific** (e.g., IG hotlines) resources for reporting fraud and **outline whistleblower** protections.
- Training content should be developed in coordination with your IG and should include specific examples of past cases and schemes to make the training more interesting and memorable.
- Training programs should include interactive sessions, such as role-playing exercises to keep participants engaged and help employees practice the thoughts and behaviors demonstrated in the training materials. Employees that have practiced antifraud skills and behaviors in a simulated environment will be more likely to use them effectively in their day-to-day work.

Play 10 - Train Your People

Checklist

- ☐ **Use** available resources to help design your antifraud training program. The Fraud Awareness Week Training Guide provides useful information and important considerations for developing an antifraud training program for your employees.
- ☐ **Define** training needs by identifying weak areas through your fraud risk assessment, audit reports and/or findings, common risks in the agency, etc.
- ☐ **Select** the target audience based on the defined training needs and include all relevant internal and external stakeholders. It can be just as effective to train external contractors and vendors as it is to train your own staff.
- ☐ **Develop** learning objectives that are specific and measurable, such as "Procurement officials will be able to walk through potential scenarios using a four-step approach to identify red flags of procurement fraud."
- ☐ **Select** the training method that works best for the target audience, such as instructor-led, online courses, webinars, or job aids. Make the training eligible for continuing professional education credits to incentivize attendance.
- ☐ **Draft** agency-specific content that educates staff about what constitutes fraud, how fraud harms everyone in the agency, and how to identify and report questionable activity.
- ☐ **Deliver** training that is interactive and engaging. Include case studies and role playing exercises to provide staff an opportunity to practice the skills and behaviors to promote learning and retention of the material.
- ☐ **Evaluate** the effectiveness and impact of the training against the stated learning objectives using an established methodology, such as a pre- and post-training survey to compare the level of understanding of the skills and concepts before and after the seminar. Adjust the training approach and materials based on the results.
- ☐ **Adapt** the training to address new fraud schemes, regulations, policies, and any other new environmental factors.
- ☐ **Promote** additional training opportunities, such as those provided by your IG office, and other resources that can educate staff about the types of fraud your agency is susceptible to.

Play 11 - Know Thyself (and Thy Agency)

Why is this important

Whether your agency is big or small, centralized or decentralized, works in silos or in a seamless manner across all divisions, it is likely that the building blocks to your antifraud efforts exist in-house. Previous efforts have identified red flags, bad actors, and information that you can use across your agency to prevent fraudsters from successfully targeting your program or agency. Having program managers and leadership share information is a valuable way to capitalize on previous efforts within your agency. Ultimately, these efforts can help in overall agency governance and help inform and assess the agency's broader fraud risk management strategy.

KEY POINTS

- **Internal information sharing can help your agency understand what has and hasn't worked** in programs within the agency's culture and resource constraints. Additionally, this can help in reviewing policies and processes and identifying vulnerabilities.
- **Other programs may have already identified the identity or traits of a fraudster** - use that to your advantage and bring together those valuable data.
- Sharing information can **help you build an agency-wide repository for bad actors and the characteristics of fraud**. Your agency's antifraud team should be responsible for this effort (see *Play 4*).
- **The GAO Fraud Risk Framework** states that combining data across programs and from separate databases within an agency is a part of an effective data analytics program (see *Play 8* and *Play 9*)
- **This process helps you at all stages** of your antifraud efforts, whether you are implementing a new effort looking to inventory capability or a long standing initiative monitoring efforts across your agency.

Play 11 - Know Thyself (and Thy Agency)

Checklist

- ☐ **Solicit** input from program managers, leadership, and other program integrity efforts across the agency on what antifraud efforts and data exist.
- ☐ **Gather** various data from across the agency in order to create a central source of fraud related information.
- ☐ **Create** a space for your colleagues to present potentially impactful ideas or initiatives that can affect the entire agency.

Illustration

Leveraging data and sharing information from across your agency could help prevent fraud. For example, in the case of one large agency that handles contracts, benefits, healthcare, and operations, sharing the names of individuals who have fraudulently obtained benefits or healthcare in one program would help prevent those individuals from obtaining benefits from other programs in the future. Additionally, fraud that has been perpetrated in the healthcare space may come with certain characteristics such as a locality, individual identity, or piece of information submitted as part of an application. That information would be valuable to know in other programs as well.

Play 12 - Sharing is Caring

Why is this important

Learning from others who are dealing with similar fraud issues can be an accelerator in your antifraud program development. Intragovernmental forums and conferences enable you to learn from your colleagues across government and share your own experiences in order to help others. Intragovernmental forums and conferences can serve to provide support for nascent efforts or foster innovation for more evolved efforts. But you don't have to wait for a conference—take the initiative to host a knowledge sharing community of practice or a round-table discussion yourself. These forums can start small and involve just a few people and grow from there.

KEY POINTS

- **Forums can be a valuable resource** to learn about successes and challenges across government.
- **Data analytics programs are better when they draw** upon the lessons learned across government instead of in just one agency.
- **Interaction among colleagues across government can bring about new initiatives** and support for antifraud programs.

Play 12 - Sharing is Caring

Checklist

- ☐ **Identify** agencies that may add to your efforts, whether those agencies are similar to yours or have a different approach to their antifraud program or efforts that could complement your current approach.
- ☐ **Use** this venue to understand what you need to do to start or evolve your analytics capabilities by learning from those who have already walked down that path. Share your own experiences with others too.
- ☐ **Solicit** input on initiatives your agency has implemented in order to obtain feedback on challenges and factors for success. For example, if various programs or offices have taken part in intergovernmental forums in the past, you can find out what has worked in making progress.
- ☐ **Create** an environment in which you and your colleagues from across government feel encouraged to share successes and failures, see value, and look forward to participating in these forums. Take part in forums your colleagues from different agencies host to share and learn, such as the OMB Fraud Working Group and Data Sharing Community of Practice.

Illustration

You can start by identifying agencies with similar missions as yours and meeting with those agencies to discuss ongoing efforts. Additionally, you could look for agencies that have similar resources and capabilities and identify ways to enhance your data analytics efforts (see *Play 8* and *Play 9*). For example, a group of agencies with science-oriented missions may consider having a forum to discuss the lessons learned on scientific grant-making. Another example of an antifraud working group is a government-wide effort on travel and purchase cards. All government agencies face challenges in these programs and can learn from one another about approaching the issues and effective data analytics tools that could help mitigate the risks. Simple data analytics (see *Play 8*) could help identify purchases made on holidays or weekends, or split purchases intended to hide the true amount of an item. These flags can then be used for further investigation. Some agencies have already implemented such tools and can help other agencies begin to build those capabilities. For additional resources on travel and purchase card fraud issues, please refer to www.oversight.gov or the Council of Inspectors General on Integrity and Efficiency website, www.ignet.gov.

Play 13 - Take What is Theirs and Make It Yours!

Why is this important

Using external data to supplement the resources within your agency is a powerful way to build your own high quality data set, creating a thorough and powerful tool in your fraud risk management arsenal. External data can give you information that you didn't know existed or you never thought to ask for, and can therefore add layers to your data analytics program that help further prevent and detect fraud. External data can also serve as a validation of findings through the correlation of multiple data sources. External data can come through data sharing agreements, use of shared analytics services such as the Do Not Pay Business Center (DNP), other agencies, third party sources such as banks, or obtaining access to state and local level data. While these agreements can take time to establish, they can also be incredibly helpful in fraud risk management.

KEY POINTS

- **Data sharing agreements** are a way to formally share data with other agencies.
- **Data sharing agreements** also help agencies create clear plans for what they will do with the data. Have a goal for the data you are looking to gain access to and a plan on how to use the data once you have it.
- **The GAO Fraud Risk Framework** states that pursuing data-sharing agreements are key elements of a data analytics program (see *Play 8* and *Play 9*) and enhance fraud risk management activities.
- **Shared analytics services have access to data and tools that you may not have access to**, providing you with valuable insight from multiple data sources.
- **State and local level data can be beneficial** and improve coordination and collaboration between federal, state, and local counterparts.

Play 13 - Take What is Theirs and Make It Yours!

KEY POINTS (continued)

- **When planning to share data** make sure you can answer the following questions:
    - Do I know what I need to do to get access to the data sources both within and outside my agency?
    - Do I understand the statutes surrounding data access and data sharing such as the Computer Matching and Privacy Protection Act or System of Records Notices?
    - Do I have an inventory of data sources within my agency and a list of sources outside the agency that will help my program(s)?
    - How will I implement new data sharing agreements or take steps to use a shared analytics resource?

Checklist

- ☐ **Identify** external data sources that may help your agency fight fraud within the various missions.
- ☐ **Understand** the potential legal or procedural steps you will have to take to access external data sources.
- ☐ **Advocate** for relevant parties in your agency, such as the General Counsel's office and IT department, to move toward establishing data sharing agreements or using shared services.
- ☐ **Update** your data sources on a routine basis so that you are always seeking out new and beneficial data sources to help you prevent and detect fraud.

Play 13 - Take What is Theirs and Make It Yours!

Illustration

Financial and non-financial agencies alike use external data to help in their missions. For example, U.S. Citizenship and Immigration Services (USCIS) works with the Financial Crimes Enforcement Network, the Federal Deposit Insurance Corporation, and the U.S. Securities and Exchange Commission to access additional data in its management of the EB-5 Immigrant Investor program. In creating these relationships and sharing data, USCIS came to appreciate some of the securities, finance, and investment aspects of the EB-5 visa program and the need to manage such a program in a manner that differed from other visa programs. The relationships yielded benefits to all parties and the agencies now support one another in investigations, training, and share information from informant tips and files when appropriate to understand better what may be happening in specific instances. This is just one example of how external data can help advance your programs. Many agencies that administer benefits look to state level data to augment their own data resources. Agencies have also touted the advantage of having a service such as DNP to help in data checks, validation, and identifying potential fraud. Finally, the Inspector General Empowerment Act of 2016 exempts IG from the Computer Matching and Privacy Protection Act. Thus, if an agency works closely with an OIG as part of a joint data analytics effort, the OIG might be able to match data to other agency data in a more streamlined manner.

Play 14 - Establish a Feedback Loop with Your IG

Why is this important

Your IG is a great resource for information related to fraud schemes, indicators, risks, and internal control deficiencies across your agency. Developing a feedback loop with your IG can provide useful information that can improve your analytics models (see *Play 8* and *Play 9*) and help improve fraud awareness (see *Play 4*), processes, and controls to identify and mitigate fraud risks.

KEY POINTS

- **Your IG is responsible for investigating, auditing, and conducting other reviews involving fraud and related vulnerabilities.** Many IGs have law enforcement authority to pursue criminal actions in coordination with prosecutors.
- **Each agency IG views the relationship with antifraud teams differently and will establish different expectations regarding the timing and involvement of your IG in potential fraud.** Agencies should consider integrating IG audits and other reviews (inspections/evaluations), as IG investigations are not the only source of information on agency fraud risks. Find a model that works for your agency and IG.
- **Details of IG reports and closed fraud investigations can provide valuable information for your analytics models** (see *Play 8* and *Play 9*). These data points help your supervised learning analytics models identify trends and patterns more effectively.
- **IG reports and closed IG investigations can provide valuable information about gaps in policies or procedures** that program office staff can use to strengthen their antifraud controls.
- **While there is a line between the IG and the agency that maintains independence, there are ways to share information to better the agency as a whole without crossing that line.** You should aim to find that balance between your agency and IG in this information sharing process.

Play 14 - Establish a Feedback Loop with Your IG

KEY POINTS (continued)

- **IG reports, investigations, and audits; annual audit plans; management challenge reports; and www.oversight.gov can all provide useful examples**, fraud schemes, and fraud indicators that can be used for your antifraud training (see *Play 3* and *Play 10*).

Checklist

- ☐ **Establish** a feedback loop with your IG to share the results of closed fraud investigations and completed audits with the antifraud and data analytics teams (see *Play 4* and *Play 9*).
  - In the development of your program, the antifraud team (see *Play 4*) should be the primary point of contact with the IG.
- ☐ **Share** information and lessons learned related to closed fraud investigations with the appropriate program offices to help improve policies, processes, and controls.
- ☐ **Promote** the outcomes of successful IG investigations to raise awareness of the schemes and emphasize the positive impact of identifying and stopping fraud.
- ☐ **Use** existing IG-provided resources. For example, your IG may have lists of common fraud schemes and red flags published on the agency's website.
- ☐ **Encourage** participation in IG antifraud events and trainings. Your agency antifraud team should communicate those opportunities to the relevant stakeholders.
- ☐ **Invite** IG representatives to speak at antifraud training and fraud awareness events.

Note: We recommend working with your OIG to define this review process and the information your OIG expects or needs when you refer a case to them. This will help you and your OIG set expectations for one another during this process. For example, you could work with your OIG to develop a checklist of information that should be provided when your agency refers a case.

Insight into Action

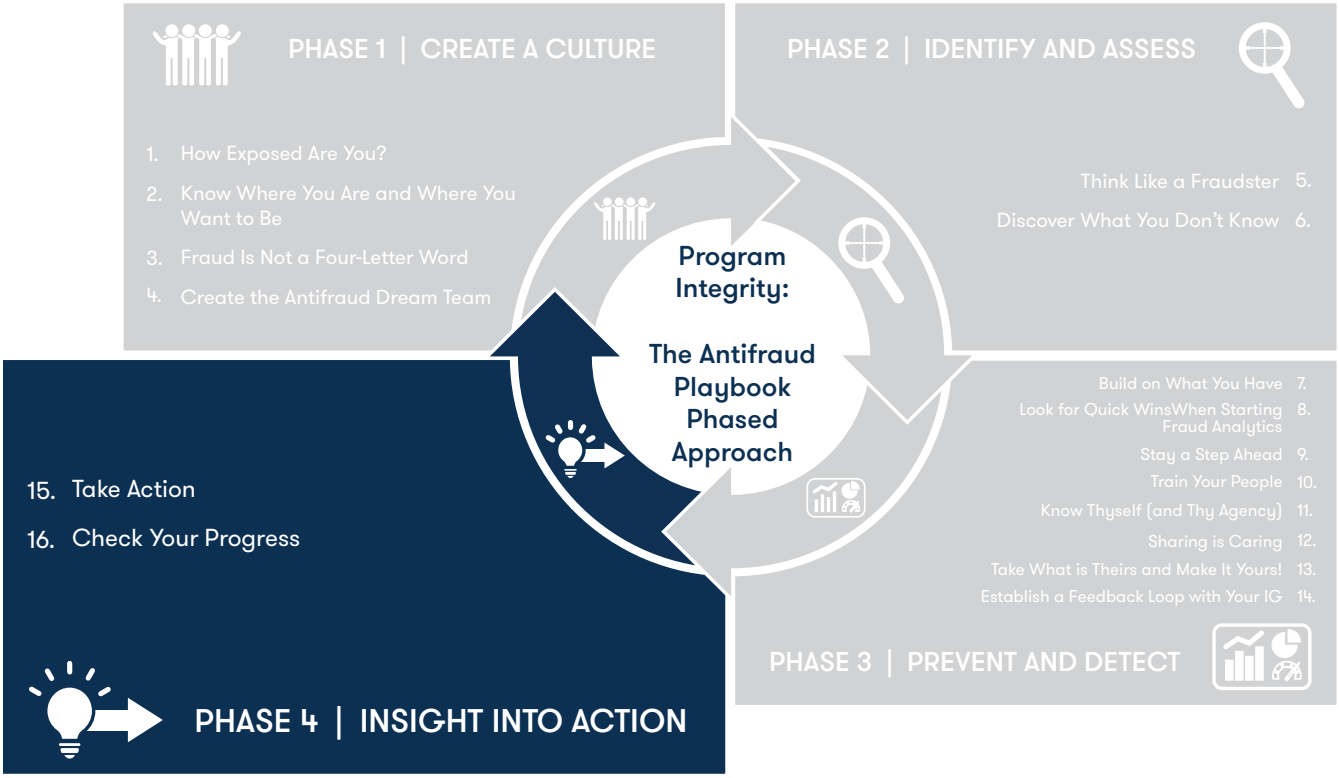


Figure 12: Four-Phased Approach, Insight into Action

Why is this important

The fourth and final phase in your antifraud journey is all about evaluating the outcomes of the fraud risk management activities and efforts you have implemented in the first three phases. In this phase, we provide guidance on two main items. We discuss how to take action against potential incidents of fraud (see *Play 15*) and how to monitor and evaluate your fraud risk management activities by measuring the outcomes of your efforts (see *Play 16*).

The two plays included within this phase will help you act upon the insights you gained in the previous phases so you begin to see progress in your agency.

What plays are included

15. Take Action
16. Check Your Progress

Play 15 - Take Action

Why is this important

You are now armed with results (see *Play 6*), analytics (see *Play 8* and *Play 9*), and insight (see *Play 11*, *Play 12*, *Play 13*, and *Play 14*), and it's time to take action. Using the insights gathered from these activities, you can now begin to tackle and prioritize potential incidents of fraud and fraud risks. While it might be difficult to measure outcomes as a result of fraud prevention tactics, measuring outcomes is a vital step to an effective and robust antifraud program and can lead to significant return on investment (ROI) (see the *'Case Study'*).

KEY POINTS

- **Insight without action is useless.**
- **The identification of potential incidents of fraud can take on many forms.** For example, you might identify a suspicious payment through your analytics efforts. Or you might receive a tip from a hotline. No matter the form, each incident is an opportunity to take action.
- Having **a plan to respond to, prioritize, and tackle potential incidents of fraud** as a result of your antifraud and integrity activities is a key component to a robust program, and is a key component to **establishing 'lessons learned.'**
- You can and should **use identified instances of fraud and fraud trends to improve fraud risk management activities** on an iterative and consistent basis.
- You can and should review and use the results of investigations and prosecutions that occur as a result of identified potential incidents of fraud to **enhance fraud prevention and detection at your agency** (see *Play 14*).
- Taking action can act as **a strong preventative technique.** It increases the perception that incidents of potential fraud are not only being identified, but are being thoroughly investigated.

Play 15 - Take Action

Checklist

- ☐ **Develop** a plan outlining how you will respond to identified instances of fraud. For example, establish a reporting process with your OIG for referring potential instances of fraud.

  Note: The process for identifying potential incidents of fraud can take on many forms (see 'Key Points'). It may be beneficial to develop a plan on how you will handle leads from the various sources as the processes and procedures may differ. For example, the process for handling an anonymous tip may be different than handling a potential incident of fraud identified through analytics. These processes might also be different from the reporting process you develop with your OIG, noted above.

- ☐ **Identify** potential incidents of fraud.

  This can be done by reviewing the results of your fraud risk assessment (see Play 6), analytics activities (see Play 8 and Play 9), or insights gathered from collected and available information (see Play 11, Play 12, Play 13, and Play 14). For further examples, see 'Key Points'.

- ☐ **Prioritize** potential incidents of fraud. The prioritization of potential incidents of fraud can be done in a number of ways. Some examples include:

  - Prioritizing potential incidents of fraud based on level of stakeholder interest or potential reputational harm, making potential incidents of fraud identified in areas with high stakeholder interest a higher priority.
  - Prioritizing potential incidents of fraud based on level of risk (see Play 6), making potential incidents of fraud found in areas that have been assessed as high risk a higher priority.

- ☐ **Review** potential incidents of fraud and refer appropriate cases to the OIG (see Play 14) or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.

  From an agency's perspective, reviewing potential incidents of fraud may include removing false positives, gathering further information, or verifying the facts and circumstances.

  Note: We recommend working with your OIG to define this review process and the information your OIG expects or needs when you refer a case to them. This will help you and your OIG set expectations for one another during this process. For example, you could work with your OIG to develop a checklist of information that should be provided when your agency refers a case.

- ☐ **Coordinate** with your IG to determine what information and support documentation they need to initiate an investigation and how that information should be shared.

Play 15 - Take Action

Checklist (continued)

*Note: When false positives are identified, ensure you take the time to investigate why a false positive occurred as it may be an opportunity to improve your fraud risk mitigation activities. For example, if the false positive was identified through your analytics activities (see **Play 8** and **Play 9**), then you can better inform your analytics model by incorporating the lesson learned from the false positive.*

- ☐ **Follow up** with the IG (see ***Play 14***).
- ☐ **Identify and disseminate** lessons learned to inform and improve fraud risk management activities.

*For example, if through these efforts you identify multiple incidents of the same fraud scheme, you should communicate the details with relevant parties to ensure processes and controls are improved moving forward. Lessons learned may require updates to training (see **Play 10**) to incorporate and disseminate this information to relevant parties.*

Play 15 - Take Action

Case Study

Veterans Benefits Administration (VBA) established an Incident Team to take a more proactive approach to fighting fraud. The Incident Team is a centralized group responsible for taking action against potential incidents of fraud. Potential incidents of fraud can come in many forms. Primarily, the Incident Team relies on program operations staff to identify potential incidents of fraud in their day-to-day work. When a staff member identifies a potential incident of fraud, they should have a detailed Standard Operation Procedure (SOP) available that prescribes the actions they need to take to escalate the incident to the Incident Team. Once the Incident Team receives notice of the incident, they too have an established process for taking action to resolve it. The Incident Team prioritizes potential incidents of fraud based on pre-determined factors, such as placing a higher level of priority on cases where there is a high indication that fraud has in fact occurred. Upon closure of a lead, the Incident Team coordinates with the appropriate program office to identify trends and disseminate lessons learned in an effort to improve fraud risk management activities across VBA. Since its inception, the team has investigated over 18,000 potential incidents of fraud and recovered over $11 million, showcasing that taking action can result in big wins.

Play 16 - Check Your Progress

Why is this important

Repeated monitoring and periodic evaluations are not only efficient methods for checking your work, but also provide insight into the effectiveness of fraud risk management activities and help you identify areas for improvement.

KEY POINTS

- **Monitoring and evaluations are proactive measures that can increase the perception of detection.** Therefore, similar to the fraud risk assessment process (see *Play 6*), the monitoring and evaluation processes should be visible and communicated throughout your agency.
- **Consider factors for setting the scope and frequency of monitoring and evaluations.** You should consider changes in the agency, its operating environment, and its control structure to determine the appropriate scope and frequency of your fraud monitoring and evaluation activities.
- **You should monitor and evaluate the effectiveness of preventative activities**, such as fraud risk assessments (see *Play 6*), antifraud training (see *Play 10*), and your analytics activities (see *Play 8* and *Play 9*).

  *Note: **To be effective, this process should focus on measuring the outcomes** of those activities **instead of simply reviewing outputs.** For example, instead of focusing on the number of fraud risk assessments performed (the output), you can measure the change in likelihood and impact scores from one assessment to the next to measure how awareness and understanding has improved those schemes since the previous assessment. For further details, see page 30 of GAO's Fraud Risk Framework.*

- As part of this process, you **should collect and analyze data from reporting mechanisms**, such as hotlines, **and instances of detected fraud**, through items such as the fraud risk assessment (see *Play 6*), analytics activities (see *Play 8* and *Play 9*), and IG investigations (see *Play 14*). This data will allow you to monitor fraud trends and provide another avenue for identifying potential internal control gaps or weaknesses.

Play 16 - Check Your Progress

KEY POINTS (continued)

- **You should use the results of monitoring and evaluations to improve fraud risk management activities at your agency.**

For example, let's say you were evaluating the level of fraud awareness (see Play 3) within a particular program after conducting targeted antifraud training (see Play 10) using a survey, and the results were lower than expected. This would indicate that the outcome of the training was not adequately achieved and that the training should be improved to achieve the desired outcome.

For further details on how to incorporate feedback and adapt fraud risk management activities based on the results of monitoring and evaluations, see pages 31 through 32 of GAO's Fraud Risk Framework.

Checklist

- ☐ **Determine** the type of monitoring and evaluation activities you would like to implement. You should consider the following recommendations:
  - This should include a mix of ongoing monitoring and separate evaluations of more targeted areas.
  - This should be comprehensive and cover the different components of your antifraud program, including awareness and training initiatives (see *Play 3* and *Play 10*), fraud risk assessments (see *Play 6*), and analytics (see *Play 8* and *Play 9*).
- ☐ **Use** existing monitoring activities, such as your agency's annual OMB Circular A-123 testing process to reduce burden on agency staff and streamline monitoring and reporting across program integrity functions (see *Play 7*).
- ☐ **Set** the scope and frequency of monitoring and evaluation activities.

For example, if you plan to conduct targeted evaluations of your training initiatives, you may decide that this should occur ad-hoc (frequency) after each occurrence of a new training program or topic (scope). This would allow you to evaluate the effectiveness of new training programs or materials and implement lessons learned based on the results of the post-training evaluation.

Play 16 - Check Your Progress

Checklist (continued)

*Note: As stated in the second bullet in **'Key Points'**, you should consider changes in the agency, its operating environment, and its control structure to determine the appropriate scope and frequency of your fraud monitoring and evaluation activities. For example, if a particular program undergoes a significant reorganization that would impact antifraud activities or risks, you may need to conduct additional evaluations until the dust settles.*

- ☐ **Establish** appropriate measurement criteria to assist in the monitoring and evaluation of fraud risk management activities.

*Note: This should focus on measuring the outcomes of fraud risk management activities vs. simply reviewing the outputs of those activities. See third bullet number under **'Key Points'** for further details.*

- ☐ **Evaluate** the results of monitoring and evaluation activities against your established measurement criteria.

*Note: See third bullet under **'Key Points'** for further details.*

- ☐ **Remediate** deficiencies identified based on the results of monitoring and evaluation activities.

For example, if you identify weaknesses in your internal controls related to identity verification in call centers, work with relevant program office staff to identify and mitigate the root cause and perform validation testing to verify the newly designed controls are operating effectively.

- ☐ **Communicate** the results of monitoring and evaluation activates to relevant stakeholders.

Note: The results of your monitoring and evaluation activities should be summarized and reported to relevant agency stakeholders. This may include both senior leadership and staff aligned to the program or business function related to the area of focus of the results. For example, if you are monitoring the fraud risk assessment process of the payroll function, you should communicate the results to both relevant senior leaders and payroll-specific personnel, including the relevant payroll system owners and human resources personnel if the issues relate to the handoff between human resources and payroll functions.

Appendix A

How does the playbook align to relevant guidance?

As explained in the Introduction, the playbook helps to clarify and operationalize the concepts put forward in other guidance, including GAO's *Framework for Managing Fraud Risks in Federal Programs* (The Fraud Risk Framework), GAO's Green Book, improper-payment legislation, and the Office of Management and Budget (OMB) circulars. Additionally, the playbook offers suggestions for integrating disparate compliance activities using your existing governance structure.

Below, we outline in detail how the playbook aligns to relevant guidance, including:

- The Fraud Risk Framework
- The Green Book
- OMB Circular No. A-123

The Fraud Risk Framework

GAO issued the Fraud Risk Framework in July 2015. The Fraud Risk Framework establishes a structure for developing an effective integrity program. The four key components of The Fraud Risk Framework are:

- **Commit**—Commit to combating fraud by creating an organizational culture and structure conducive to fraud risk management.
- **Assess**—Plan regular fraud risk assessments and assess risks to determine a fraud risk profile.
- **Design and Implement**—Design and implement a strategy with specific control activities to mitigate assessed fraud risks and collaborate to help ensure effective implementation.
- **Evaluate and Adapt**—Evaluate outcomes using a risk based approach and adapt activities to improve fraud risk management.

Each of these components aligns to a phase and a related set of plays within this playbook, see *Figure 13*.

Appendix A (continued)

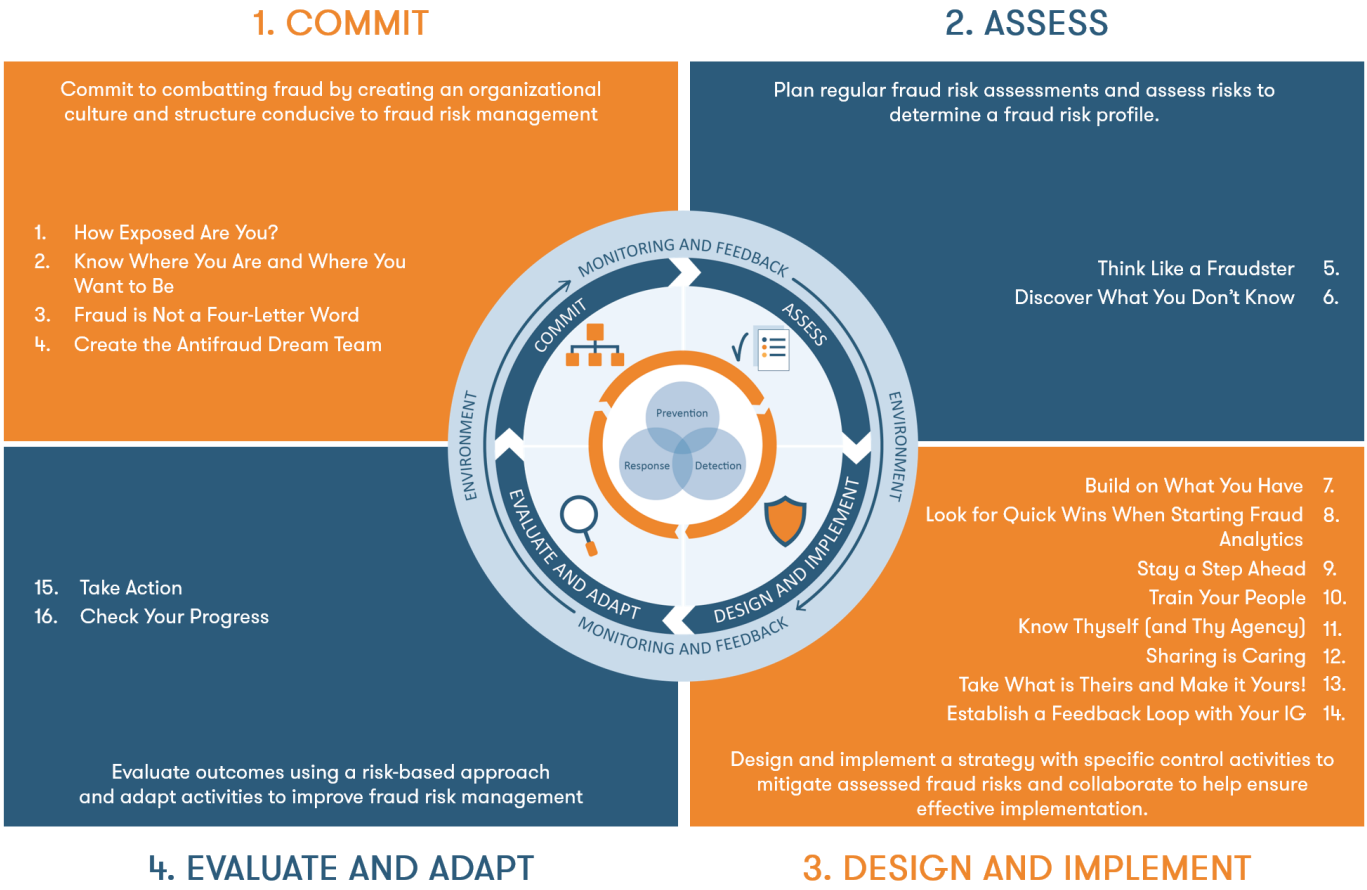


Figure 13: GAO's Fraud Risk Framework and the Antifraud Playbook

Figure 13 provides a high-level overview of how the Playbook aligns to the Fraud Risk Framework. To provide further context, we have developed a detailed crosswalk to display how each play aligns to the components and sub-components within the Fraud Risk Framework.

You can use this crosswalk to better understand how the Playbook aligns to the Fraud Risk Framework, and to better understand what elements of the Fraud Risk Framework you are working towards adopting as you complete the plays. Further, as displayed, completing the checklist items included in each play will help your adopt the practices within the different components of the Fraud Risk Framework.

Click here to access the crosswalk.

Fraud Risk Assessment

The Fraud Risk Framework outlines five key elements of the fraud risk assessment process, which include:

- **Identify inherent fraud risks affecting the program**—Managers determine where fraud can occur and the types of fraud the program faces, such as fraud related to financial reporting, misappropriation of assets, or corruption. Managers may consider factors that are specific to fraud risks, including incentives, opportunity, and rationalization to commit fraud.
- **Assess the likelihood and impact of inherent fraud risks**—Managers conduct quantitative or qualitative assessments, or both, of the likelihood and impact of inherent risks, including the impact of fraud risks on the program's finances, reputation, and compliance. The specific methodology managers use to assess fraud risks can vary by program because of differences in missions, activities, capacity, and other factors.
- **Determine fraud risk tolerance**—According to Standards for Internal Control in the Federal Government, a 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.
- **Examine the suitability of existing fraud controls and prioritize residual fraud risks**—Managers consider the extent to which existing control activities mitigate the likelihood and impact of inherent risks. The risk that remains after inherent risks have been mitigated by existing control activities is called residual risk. Managers then rank residual fraud risks in order of priority, using the likelihood and impact analysis, as well as risk tolerance, to inform prioritization.
- **Document the program's fraud risk profile**—Effectively assessing fraud risks involves documenting the key findings and conclusions from the actions above, including the analysis of the types of fraud risks, their perceived likelihood and impact, risk tolerance, and the prioritization of risks.

Keeping these five key elements in mind, we developed practical and actionable checklist items (see *Play 6*) that agencies can take within each of the elements outlined in the Fraud Risk Framework for an effective fraud risk assessment. These checklist items will help you develop, implement, or expand your current fraud risk assessment efforts. Additionally, we have developed a graphic to further illustrate how the checklist items in Play 6 align to these five key elements (see *Figure 14*).

The Green Book

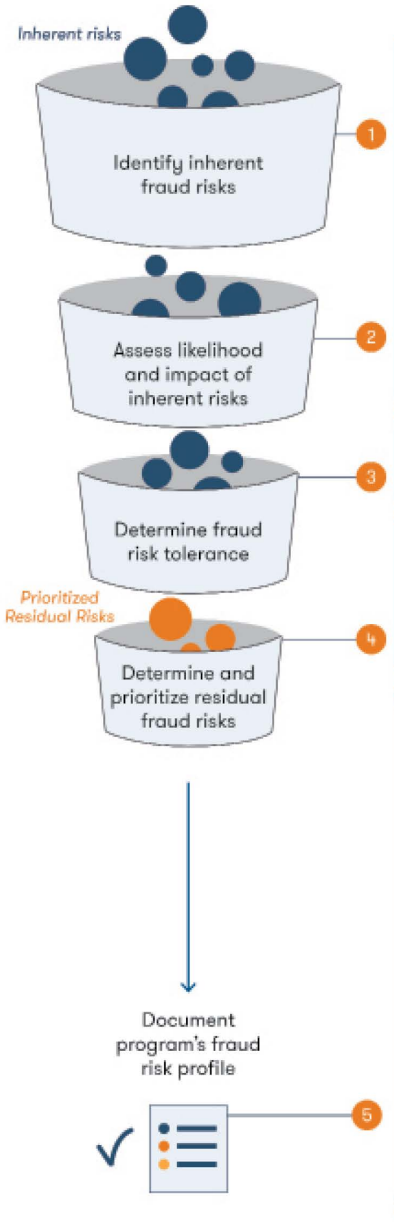
GAO released the Green Book in September 2014 and it provides criteria to federal program managers for designing, implementing, and operating an effective internal control system. Federal program managers must adhere to the five components and 17 principles that make up the Green Book. While all principles are important for creating an internal control environment that is conducive to preventing and detecting fraud, principle 8 provides specific guidance to agencies related to assessing fraud risks.

Below is a crosswalk that aligns the plays introduced in the Antifraud Playbook to the Green Book attributes for principle 8 - *Assess Fraud Risks*. Principle 8 is comprised of seven primary attributes, including:

GAO Green Book to Antifraud Playbook Crosswalk	
Green Book Attribute	**Play**
Management should consider the potential for fraud when identifying, analyzing, and responding to risks. (8.01)	• Play 6 – Discover What You Don't Know
Management considers the types of fraud that can occur within the entity to provide a basis for identifying fraud risks. (8.02)	• Play 5 – Think Like a Fraudster • Play 6 – Discover What You Don't Know
In addition to fraud, management considers other forms of misconduct that can occur, such as waste and abuse. (8.03)	• *Play 6 – Discover What You Don't Know (* See note below)*
Management considers fraud risk factors, including incentive/pressure, opportunity, and attitude/rationalization. (8.04)	• Play 5 – Think Like a Fraudster • Play 6 – Discover What You Don't Know
Management uses the fraud risk factors to identify fraud risks. (8.05)	• Play 6 – Discover What You Don't Know
Management analyzes and responds to identified fraud risks so that they are effectively mitigated. (8.06)	• Play 6 – Discover What You Don't Know
Management responds to fraud risks through the same risk response process performed for all analyzed risks. (8.07)	• Play 6 – Discover What You Don't Know • Play 7 – Build on What You Have

**Note: While the playbook specifically addresses fraud, efforts to identify, assess, and mitigate fraud risks will also help manage waste and abuse.*

PLAY 6 CHECKLIST ALIGNED TO GAO FRAUD RISK FRAMEWORK



- ☐ **Identify** the following:
  - Your preferred approach or unit of analysis
  - Your starting point within your unit of analysis, i.e., the specific program(s) or function(s) you plan to assess first
- ☐ **Use** your Fraud Risk Map to identify the types of internal and external fraud risks your chosen starting point faces.
- ☐ **Identify** your preferred risk assessment technique or techniques and
  - **gather** information on the controls and processes in place;
  - **determine** if and how the controls and processes in place could be exploited or circumvented; and
  - **assess** the likelihood and impact of given schemes being successful.
- ☐ **Document** the results of your risk assessment.
- ☐ **Translate** the fraud schemes into specific risks.

- ☐ **Determine** your fraud risk tolerance.

- ☐ **Prioritize** risks based on the results of the assessment and your fraud risk tolerance.
- ☐ **Develop** responses to mitigate the likelihood and impact of risks, including the identification of "owners" for each response activity. Responding to fraud risks is imperative to successful and effective fraud risk management.

- ☐ **Document** the fraud risk profile. Called for in GAO's Fraud Risk Framework, a fraud risk profile is essentially a summary of the outputs of the fraud risk assessment process and should at a minimum include the high priority fraud schemes, likelihood and impact, risk tolerance, risk prioritization, response activity, and owner.
- ☐ **Report** the results. The results of your fraud risk assessment should be summarized and reported to relevant agency stakeholders. Note that sharing information about your fraud risk tolerance outside the agency or outside senior leadership within the agency is not necessary and may not be advisable. Hesitance to share this information should not be cause for failing to conduct the analysis.
- ☐ **Evaluate** the effectiveness of your risk assessment and make changes to the process based on lessons learned, successes, and pitfalls.
- ☐ **Repeat and update** this process for the selected assessable unit iteratively as you learn and as your efforts mature. A fraud risk assessment is not a "one-and-done" activity. You will have to periodically re-conduct the fraud risk assessment for each assessable unit.
- ☐ **Expand** the risk assessment to other areas, or assessable units, based on your preferred approach.
- ☐ **Aggregate** results for each assessable unit in which you conduct a risk assessment to develop an agency-level view of your fraud risk and identify trends.

To see the original version of this graphic, see page 16 of GAO's Fraud Risk Framework.

NOTE: This is a pared-down version of the checklist to include only the key checklist items. For the full details of this checklist, which includes examples and additional resources, plee see Play 6.

Figure 13: GAO's Fraud Risk Framework and the Antifraud Playbook

OMB Circular A-123

OMB Circular A-123 (M-16-17) has long been the foundation of federal requirements related to accountability, efficiency, and effectiveness of government program operations. OMB released the revised Circular A-123 (M-16-17) in July 2016, which requires agencies to implement enterprise risk management (ERM) programs in coordination with their internal control processes required by FMFIA and GAO's Green Book. The purpose of the revised circular was to encourage an integrated governance structure meant to improve mission delivery, reduce costs, and focus corrective actions towards key program risks. The Antifraud Playbook was developed with this approach in mind, providing guidance to agencies to help implement an antifraud program that is integrated with other ongoing risk management initiatives.

OMB Circular A-123 (M-16-17) addresses fraud risk in section B.2: Managing Fraud Risks in Federal Programs. This section outlines requirements to agencies related to the following areas:

- Defines fraud, waste, and abuse using the GAO Green Book definitions for each term.
- Requires that an agency's risk profile include an evaluation of fraud risks and use a risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks. "The financial and administrative controls established through the agency's risk profile must also include:
    - controls to address identified fraud risks related to payroll, beneficiary payments, grants, large contracts, information technology and security, asset safeguards, and purchase, travel and fleet cards;
    - collecting and analyzing data from reporting mechanisms on detected fraud to monitor fraud trends and using that data and information to continuously improve fraud prevention controls; and
    - using the results of monitoring, evaluation, and investigations to improve fraud prevention, detection, and response.
- States that agencies should adhere to the leading practices of GAO's Fraud Risk Framework to effectively design, implement, and operate an internal control system that addresses fraud risk. Specifically, OMB Circular A-123 (M-16-17) states:

> "To help managers to combat fraud and preserve integrity in government agencies and programs, GAO identified leading practices for managing fraud risks and organized them into a conceptual framework called the Fraud Risk Management Framework (the Framework, GAO-15-593SP). Managers should adhere to these leading practices as part of their efforts to effectively design, implement, and operate an internal control system that addresses fraud risks. Managers are responsible for determining the extent to which the leading practices in the Framework are relevant to their program and for tailoring the practices, as appropriate, to align with the program's operations."

Similar to the GAO Fraud Risk Framework and OMB Circular A-123 (M-16-17), the Antifraud Playbook provides guidance to agencies that emphasizes prevention as the most effective means of addressing fraud in government programs (see *Play 3*, *Play 6*, *Play 8*, and *Play 9*). The playbook also highlights the importance of monitoring and adapting your program to address identified weaknesses in the control environment and antifraud efforts (see *Play 16*). By implementing the plays provided in this playbook, agencies will make significant progress towards addressing requirements outlined in OMB Circular A-123 (M-16-17).

OMB Circular A-123, Appendix C

OMB released a revision to Circular A-123, Appendix C (M-18-20) in June 2018 that seeks to "transform the improper payment compliance framework into a more unified, comprehensive, and less burdensome set of requirements." The idea of integrating compliance activities aligns well to the Antifraud Playbook, *Play 7 – Build on What You Have*. Beyond the goal of streamlining program integrity activities, the following points help align the Antifraud Playbook to the revised OMB Circular A-123, Appendix C –

- **Fraud as a subset of improper payment.** Appendix C states that improper payments fall into three broad categories—intentional fraud and abuse, unintentional payment errors, and instances where the documentation for a payment is insufficient to determine whether a payment is proper. Based on the categories provided by OMB and as highlighted in the Antifraud Playbook Introduction, the Playbook makes it clear that fraud is considered a subset of improper payments. Therefore, OMB advises that your annual Improper Payments

Elimination and Recovery Improvement Act (IPERIA) activities may uncover transactions that are anomalous or indicative of potential fraud and should be referred to your IG or the Department of Justice for further investigation. Further, OMB states, "transactions should not be categorized as fraud until the appropriate judicial or adjudicative process makes the determination. The circumstances contributing to the anomalous transaction could indicate an internal control weakness that resulted in a mistake that should be analyzed by management and, if necessary, corrected." Based on this guidance, *Play 15* and *Play 16* provide agencies with key points and checklists to help take action to address suspicious transactions when they are uncovered and carry out remediation activities when your monitoring processes identify potential control weaknesses that could allow fraud to occur.

- **Connecting fraud, improper payments, and ERM.** An ERM framework should provide an enterprise-wide, strategically aligned view of organizational challenges and risks that can help agency management prioritize resource allocations to ensure successful mission delivery. Agencies should use their ERM frameworks to effectively manage fraud risk and ensure the integrity of federal payments, which is fundamental to the core mission for agencies. The Antifraud Playbook provides practical guidance to help agencies implement and improve processes to identify and mitigate financial and non-financial fraud risks that could affect the agency's strategic, operational, reporting, and compliance objectives.

Similar to OMB Circular A-123 Appendix C, the Antifraud Playbook provides guidance to agencies that emphasizes the importance of managing fraud risk as a method to reduce the potential impact of fraud. Further, analyzing why a potential incident of fraud occurred and incorporating lessons learned from that incident (see *Play 14* and *Play 15*), such as improving internal controls, is a key focus and recommendation in the Antifraud Playbook.

Appendix B

Checklist Repository

Looking for a simple way to access all the checklists within the playbook in one place? You have come to the right appendix. Below we have included each checklist in the playbook, broken out by phase and by play, for your reference and convenience.

You can select the phase or play you would like to see from the list below, which will automatically navigate you to your selected phase or play.

Click here for a printable version of this Appendix.

The Plays

Create a Culture

1. How Exposed Are You?
2. Know Where You Are and Where You Want to Be
3. Fraud is Not a Four-Letter Word
4. Create the Antifraud Dream Team

Identify and Assess

5. Think Like a Fraudster
6. Discover What You Don't Know

Prevent and Detect

7. Build on What You Have
8. Look for Quick Wins When Starting Fraud Analytics
9. Stay a Step Ahead
10. Train Your People
11. Know Thyself (and Thy Agency)
12. Sharing is Caring
13. Take What is Theirs and Make It Yours!
14. Establish a Feedback Loop with Your IG

Insight into Action

15. Take Action
16. Check Your Progress

CREATE A CULTURE

Play 1 - How Exposed are You?

- ☐ **Identify** the major fraud risk factors in the primary missions of your agency. Use existing documentation, knowledge, IG or GAO audits, or interviews to gather this information.
- ☐ **Determine** the weight of those factors relative to each other based on which are of greatest concern.
- ☐ **Quantify** the risk factors by determining the level to which they expose the program to fraud.
- ☐ **Use** this exercise to focus your efforts on those programs and areas that are most susceptible to fraud.

Play 2 - Know Where You are and Where You Want to Be

- ☐ **Review** the Antifraud Program Maturity Model.
- ☐ **Tailor** the bullets to fit the unique circumstances and strategic goals of your agency as needed.
- ☐ **Evaluate** your agency's current antifraud efforts.
- ☐ **Identify** your agencies 'goal state' based on your current level of maturity (see *the Antifraud Program Maturity Model*), fraud exposure (see *Play 1*), and other key factors such as agency size (see *'Key Points'*).
- ☐ **Pinpoint** the gaps between your current level of maturity and your goal state.
- ☐ **Recognize** and consider the environmental factors that could impact the achievement of your goal state, such as political, legislative, resources, etc.
- ☐ **Develop** a "road map" for how you will reach your goal state, considering the environmental factors identified in the previous step.

Play 3 - Fraud Is Not a Four-Letter Word

- ☐ **Coordinate** with your IG to develop materials, such as red flags, checklists, brochures, and posters, to support fraud awareness that describe potential fraud and fraud risks.
- ☐ **Host** a fraud awareness event or activity that occurs periodically and involves all levels of the agency, including participation from the IG. For example:
    - The Association of Certified Fraud Examiners (ACFE) hosts Fraud Week (usually in November) as a spearhead for building fraud awareness.
    - Hold fraud-focused events such as a fraud knowledge contest to challenge your coworkers to a game of who knows the most about infamous fraud cases.
- ☐ **Publicize** information on antifraud efforts and successfully resolved cases to raise awareness about program integrity and antifraud efforts outside the program.
- ☐ **Weave** frequent fraud discussions into your daily activities, such as discussing fraud topics during regularly scheduled conference calls or meetings with key stakeholders.

Play 4 - Create the Antifraud Dream Team

- ☐ **Establish** an antifraud team comprised of the right individuals to execute the agency's antifraud strategy, using the guidance outlined in *'Key Points'*.
- ☐ **Develop** clearly defined antifraud team roles and responsibilities.
    - **Coordinate** roles and responsibilities with the agency IG's office, which handles investigations (see *Play 14*).
- ☐ **Assess** fraud risks across the organization (see *Play 6*) by overseeing the fraud risk assessment process.
- ☐ **Coordinate** across business units to streamline risk management activities (e.g., internal controls, improper payments, enterprise risk management) and develop fraud risk responses and mitigation activities.
- ☐ **Communicate** to raise fraud awareness across your agency and establish relationships with program offices.
- ☐ **Train**—develop and deliver antifraud training and fraud-awareness campaigns by leveraging the guidance provided in *Play 3* and *Play 10*. Frequent training can help address the challenge of dealing with evolving, sophisticated fraud schemes.

IDENTIFY AND ASSESS

Play 5 - Think Like a Fraudster

- ☐ **Identify Internal Fraud Schemes.** For example, actors to consider include, but are not limited to:
    - Payroll Staff
    - COs / CORs
    - Management
    - Purchase or Travel Card Holders

If you have trouble identifying internal fraud schemes, you can consult external and intergovernmental sources for ideas. For example, the ACFE's Fraud Tree outlines the complete classification of internal fraud. You can review the Fraud Tree and identify any internal fraud schemes that your agency might be at risk for, such as theft, misuse of assets, or bribery.

- ☐ **Identify External Fraud Schemes.** For example, you can start this process by identifying the different actors external to your organization that may commit fraud such as:
    - Grantees
    - Medical Providers
    - Beneficiaries (and fraudsters posing as beneficiaries)
    - Contractors

Appendix B (continued)

Play 5 - Think Like a Fraudster (continued)

If you have trouble identifying external fraud schemes, you can consult external and intergovernmental sources for ideas. For example, the Association of Government Accountant's (AGA's) Fraud Prevention Tool outlines resources by business process, program area, and fraud type. Under each option, the AGA outlines risks, fraud schemes, red flags, and best practices/resources. Note: This resource can also be utilized to identify internal fraud schemes (see the first checklist item).

- □ **Develop a Fraud Risk Map.** With the help of research, prior IG and GAO findings, brainstorming, and available external and intergovernmental resources, develop a comprehensive 'Fraud Risk Map', illustrated below, to understand the potential entry points for fraud within your agency.

*Note: The Fraud Risk Map is intended to be a starting point, which will form the foundation of your fraud risk assessment (see **Play 6**).*

Play 6 - Discover What You Don't Know

- □ **Identify** the following:
  - Your preferred approach or unit of analysis (see *'Key Points'*).
  - Your starting point within your unit of analysis, i.e., the specific program(s) or function(s) you plan to assess first.
- □ **Use** your Fraud Risk Map (see *Play 5*) to identify the types of internal and external fraud risks your chosen starting point faces.
- □ **Identify** your preferred risk assessment technique or techniques (see *'Key Points'*) and
  - **gather** information on the controls and processes in place;
  - **determine** if and how the controls and processes in place could be exploited or circumvented; and
  - **assess** the *likelihood and impact* of given schemes being successful.

Keep in mind that using more than one technique will yield better results, since each technique comes with its own benefits and may provide different types of information. For example, you can design and administer a survey that gauges perceptions about the strength of the antifraud culture of your agency, which can be helpful to understand where management and staff may have different views of the culture. You can also conduct focus groups with stakeholders to discuss the controls and processes in place related to the fraud schemes identified, the strength of those controls, and the potential likelihood and impact of the schemes. These will provide different lenses in looking at your fraud risks.

Note: When assessing likelihood and impact, the specific methodology you choose to use is up to you and will vary based on differences in missions, activities, resources, expertise, and/or other factors. For further discussion on this topic, reference pages 14-15 of GAO's Fraud Risk Framework.

Play 6 - Discover What You Don't Know (continued)

- ☐ **Document** the results of your risk assessment. This includes documenting items such as the likelihood and impact score, the existing controls, or any identified gaps. For example, you can document final likelihood and impact scores for given fraud schemes in addition to any identified controls gaps in your Fraud Risk Map. See the *'Fraud Risk Mapping Exercise (Part 2)'* for an example of how you can document this information.

- ☐ **Translate** the fraud schemes into specific risks. For example, if the fraud scheme you were discussing related to a contractor overbilling for services, the specific risks you may identify include:
  - Contractors bill for goods or services that were not provided, which results in financial loss to the agency.
  - Contractors overbill for goods or services that were provided, which results in financial loss to the agency.

  These specific risks should align to the fraud schemes assessed, but call out the specific risk associated with the scheme. In the examples above, the risk we identified was financial loss, but it can be anything you may discuss or identify in your assessment as a potential risk to your agency of the particular fraud scheme.

- ☐ **Determine** your fraud risk tolerance (see the *'Fraud Risk Tolerance: Quick Tip!'* for further details).

- ☐ **Prioritize** risks based on the results of the assessment and your fraud risk tolerance. For example, you can prioritize risks based on likelihood and impact scores or strategic priorities. No matter how you decide to prioritize risks, ensure that you consider the extent to which control activities currently in place mitigate the likelihood and impact of risks and whether the remaining risk after considering those control activities exceed your fraud risk tolerance.

- ☐ **Develop** responses to mitigate the likelihood and impact of risks, including the identification of "owners" for each response activity. Responding to fraud risks is imperative to successful and effective fraud risk management.

  When responding to risks, you have a few options as defined in the Green Book:
  - ***Accept** - No action is taken to respond to the risk based on the insignificance of the risk.*
  - ***Avoid** - Action is taken to stop the operational process or the part of the operational process causing the risk.*
  - ***Reduce** - Action is taken to reduce the likelihood or magnitude of the risk.*
  - ***Share** - Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.*

  You may find a particular type of risk requires the following:
  - ***Combination Approach**—A particular risk may require more than one response activity to address certain aspects of the risk, such as accepting part of the risk and reducing another element of the risk through the implementation of additional control activities.*

Play 6 - Discover What You Don't Know (continued)

It is important to note that if you choose to "accept" a risk, there will be no mitigating actions developed. For example, you may decide to allocate resources to mitigate fraud risks identified that exceed your fraud risk tolerance level. However, for fraud risks that were determined to be unlikely or low-impact or for risks that fall within your fraud risk tolerance level, you may decide to "accept" these fraud risks and take no further action. Be sure to document your process and rationale for taking no action.

However, if you choose one of the other response activities, you will have to design and implement specific mitigation and/or control activities to respond to the specific fraud risks, which will in turn assist in the prevention and detection fraud at your agency.

- □ **Document** the fraud risk profile. Called for in GAO's Fraud Risk Framework, the fraud risk profile is essentially a summary of the outputs of the fraud risk assessment process and should at a minimum include the high priority fraud schemes, likelihood and impact, risk tolerance, risk prioritization, response activity, and owner.

You should develop a separate fraud risk profile for each unit of analysis (see 'Key Points'). For example, if your unit of analysis is at the program level then each program would have a tailored fraud risk profile upon completion of its fraud risk assessment. This could then be rolled-up to the agency level to gain an enterprise-wide view.

- □ **Report** the results. The results of your fraud risk assessment should be summarized and reported to relevant agency stakeholders. Note that sharing information about your fraud risk tolerance outside the agency or outside senior leadership within the agency is not necessary and may not be advisable. Hesitance to share this information should not be cause for failing to conduct the analysis.
- □ **Evaluate** the effectiveness of your risk assessment and make changes to the process based on lessons learned, successes, and pitfalls.
- □ **Repeat and update** this process for the selected assessable unit iteratively as you learn and as your efforts mature. A fraud risk assessment is not a 'one-and-done' activity, you will have to periodically re-conduct the fraud risk assessment for each assessable unit.
- □ **Expand** the risk assessment to other areas, or assessable units, based on your preferred approach.
- □ **Aggregate** results for each assessable unit in which you conduct a risk assessment to develop an agency level view of your fraud risk and identify trends.

PREVENT AND DETECT

Play 7 - Build on What You Have

- ☐ **Solicit** input from program managers and leadership on what kind of fraud efforts would be most useful to them.
- ☐ **Identify** other efforts you could learn from or expand upon, and coordinate with the leaders of those efforts to consolidate them. These leaders may also have insights to consider as you move forward.
- ☐ **Create** a communication strategy that conveys these consolidation efforts throughout your agency. Work with the antifraud team in this and other efforts (see *Play 4*).

Play 8 - Look for Quick Wins When Starting Fraud Analytics

- ☐ **Identify** your starting point (see *'Key Points'*).
- ☐ **Identify** all available data associated with your starting point. For example, if you are targeting purchasing or procurement fraud, you may focus on available vendor data.
- ☐ **Identify** an analytics model or set of tests that is best suited for your targeted area. Common and more simplistic analytics models to consider include:
    - **Rule-based**—As described above, this is a transaction-level technique to prevent common fraud based on known patterns. Rule-based analytics focuses on transactional data which does not adhere to organizationally accepted rules. This technique results in the identification of departures from expected procedures for additional investigation.

For example, purchase cards cannot be used to purchase alcohol (the "rule") so identifying purchase card transactions for alcohol sales would be a "rule break" and would be flagged.

- **Anomaly detection**—As described above, this technique focuses on investigating aggregate-level transactions to identify outliers compared to peer groups based on unknown patterns among common and criminal fraudsters. This type of analytics technique can help the agency learn the patterns in the data that may suggest fraud. This will allow you to identify aggregate abnormal patterns that don't conform to established normal behaviors, i.e., outliers.

For example, if a physician is charging for more than 24 hours in a day, this would be flagged as an abnormal billing pattern.

You may also consider common analytics tests as part of this process. For example, if you are targeting purchasing or procurement fraud, you could perform the following analytics test with available data:

- Look for one-time vendors or vendors with expedited payments.
- Compare purchases by ordering clerk for each vendor and product to identify vendor preference patterns.
- Compare employee names, addresses, and account information to vendor master information to identify potential conflicts of interests or hidden relationships.

Play 9 - Stay a Step Ahead

- ☐ **Use** your early analytics efforts and results (see *Play 8*) to identify a starting point for implementing more advanced analytics capabilities, perhaps focusing on areas of higher risk (see *Play 6*), areas with large volumes of available data, or fraud schemes or patterns that emerged from your early analytics tests.
- ☐ **Determine** which analytics model(s) is best suited for your targeted area. More evolved analytics models to consider include:
    - **Predictive Analytics**: As described above in Play 8, this technique can identify unobserved attributes that lead to suspicion of fraud based on known cases of fraud. For example, the analytics model could automatically reject a payment when the existence of a number of known fraudulent characteristics is present. Typically predictive analytics are using machine learning techniques, rather than flagging transactions for follow up investigation.
    - **Network / Link Analytics**: As described above in Play 8, this technique can be useful in uncovering organized fraud and associations between fraudsters by using social network analytics, looking at linked patterns for investigation and discovery. For example, an individual may not be suspicious on his or her own, but when submitted to link analysis, his or her known associates could be engaged in well-known fraud schemes which would merit further scrutiny.
    - **Text Analytics**: As described above in Play 8, this technique can parse reviews and information for red flags of fraud looking at text patterns.
- ☐ **Implement** your chosen analytics model(s) and test(s).
- ☐ **Review** the results and refer appropriate cases to the OIG for further investigation.
- ☐ **Identify and report** findings and recommendations based on the results to relevant stakeholders.
- ☐ **Evaluate** the effectiveness of your analytics model(s) and test(s) in detecting and preventing fraud.
- ☐ **Repeat and update** this process iteratively as you learn from your analytics model and tests and as your efforts mature.
- ☐ **Expand** your analytics to other areas, such as other high risk areas identified through your fraud risk assessment and/or by targeting additional common fraud scenarios (see *'Key Points'*).

Play 10 - Train Your People

- ☐ **Use** available resources to help design your antifraud training program. The Fraud Awareness Week Training Guide provides useful information and important considerations for developing an antifraud training program for your employees.
- ☐ **Define** training needs by identifying weak areas through your fraud risk assessment, audit reports and/or findings, common risks in the agency, etc.
- ☐ **Select** the target audience based on the defined training needs and include all relevant internal and external stakeholders. It can be just as effective to train external contractors and vendors as it is to train your own staff.
- ☐ **Develop** learning objectives that are specific and measurable, such as "Procurement officials will be able to walk through potential scenarios using a four-step approach to identify red flags of procurement fraud".
- ☐ **Select** the training method that works best for the target audience, such as instructor-led, online courses, webinars, or job aids. Make the training eligible for continuing professional education credits to incentivize attendance.
- ☐ **Draft** agency-specific content that educates staff about what constitutes fraud, how fraud harms everyone in the agency, and how to identify and report questionable activity.
- ☐ **Deliver** training that is interactive and engaging. Include case studies and role playing exercises to provide staff an opportunity to practice the skills and behaviors to promote learning and retention of the material.
- ☐ **Evaluate** the effectiveness and impact of the training against the stated learning objectives using an established methodology, such as a pre- and post-training survey to compare the level of understanding of the skills and concepts before and after the seminar. Adjust the training approach and materials based on the results.
- ☐ **Adapt** the training to address new fraud schemes, regulations, policies, or any other new environmental factors.
- ☐ **Promote** additional training opportunities, such as those provided by your IG office, and other resources that can educate staff about the types of fraud your agency is susceptible to.

Play 11 - Know Thyself (and Thy Agency)

- ☐ **Solicit** input from program managers, leadership, and other program integrity efforts across the agency on what antifraud efforts and data exist.
- ☐ **Gather** various data from across the agency in order to create a central source of fraud related information.
- ☐ **Create** a space for your colleagues to present potentially impactful ideas or initiatives that can affect the entire agency.

Play 12 - Sharing Is Caring

- ☐ **Identify** agencies that may add to your efforts, whether those agencies are similar to yours or have a different approach to their antifraud program or efforts that could complement your current approach.
- ☐ **Use** this venue to understand what you need to do to start or evolve your analytics capabilities by learning from those who have already walked down that path. Share your own experiences with others too.
- ☐ **Solicit** input on initiatives your agency has implemented in order to obtain feedback on challenges and factors for success. For example, if various programs or offices have taken part in intergovernmental forums in the past, you can find out what has worked in making progress.
- ☐ **Create** an environment in which you and your colleagues from across government feel encouraged to share successes and failures, see value, and look forward to participating in these forums. Take part in forums your colleagues from different agencies host to share and learn, such ase the OMB Fraud Working Group and Data Sharing Community of Practice.

Play 13 - Take What is Theirs and Make It Yours!

- ☐ **Identify** external data sources that may help your agency fight fraud within the various missions.
- ☐ **Understand** the potential legal or procedural steps you will have to take to access external data sources.
- ☐ **Advocate** for relevant parties in your agency, such as the General Counsel's office and IT department, to move toward establishing data sharing agreements or using shared services.
- ☐ **Update** your data sources on a routine basis so that you are always seeking out new and beneficial data sources to help you prevent and detect fraud.

Play 14 - Establish a Feedback Loop with Your IG

- ☐ **Establish** a feedback loop with your IG to share the results of closed fraud investigations and completed audits with the antifraud and data analytics teams (see *Play 4* and *Play 9*).
    - In the development of your program, the antifraud team (see *Play 4*) should be the primary point of contact with the IG.
- ☐ **Share** information and lessons learned related to closed fraud investigations with the appropriate program offices to help improve policies, processes, and controls.
- ☐ **Promote** the outcomes of successful IG investigations to raise awareness of the schemes and emphasize the positive impact of identifying and stopping fraud.

Play 14 - Establish a Feedback Loop with Your IG (continued)

- ☐ **Use** existing IG-provided resources. For example, your IG may have lists of common fraud schemes and red flags published on the agency's website.
- ☐ **Encourage** participation in IG antifraud events and trainings. Your agency antifraud team should communicate those opportunities to the relevant stakeholders.
- ☐ **Invite** IG representatives to speak at antifraud training and fraud awareness events.

Play 15 - Take Action

- ☐ **Develop** a plan outlining how you will respond to identified instances of fraud. For example, establish a reporting process with your OIG for referring potential instances of fraud.

  Note: The process for identifying potential incidents of fraud can take on many forms (see 'Key Points'). It may be beneficial to develop a plan on how you will handle leads from the various sources as the processes and procedures may differ. For example, the process for handling an anonymous tip may be different than handling a potential incident of fraud identified through analytics. These processes might also be different from the reporting process you develop with your OIG, noted above.

- ☐ **Identify** potential incidents of fraud.

  This can be done by reviewing the results of your fraud risk assessment (see Play 6), analytics activities (see Play 8 and Play 9), or insights gathered from collected and available information (see Play 11, Play 12, Play 13, and Play 14). For further examples, see 'Key Points'.

- ☐ **Prioritize** potential incidents of fraud. The prioritization of potential incidents of fraud can be done in a number of ways. Some examples include:

  - Prioritizing potential incidents of fraud based on level of stakeholder interest or potential reputational harm, making potential incidents of fraud identified in areas with high stakeholder interest a higher priority.
  - Prioritizing potential incidents of fraud based on level of risk (see Play 6), making potential incidents of fraud found in areas that have been assessed as high risk a higher priority.

- ☐ **Review** potential incidents of fraud and refer appropriate cases to the OIG (see Play 14) or other appropriate parties, such as law-enforcement entities or the Department of Justice, for further investigation.

  From an agency's perspective, reviewing potential incidents of fraud may include removing false positives, gathering further information, or verifying the facts and circumstances.

  Note: We recommend working with your OIG to define this review process and the information your OIG expects or needs when you refer a case to them. This will help you and your OIG set expectations for one another during this process. For example, you could work with your OIG to develop a checklist of information that should be provided when your agency refers a case.

Play 15 - Take Action (continued)

*Note: When false positives are identified, ensure you take the time to investigate why a false positive occurred as it may be an opportunity to improve your fraud risk mitigation activities. For example, if the false positive was identified through your analytics activities (see **Play 8** and **Play 9**), then you can better inform your analytics model by incorporating the lesson learned from the false positive.*

- □ **Follow up** with the IG (see ***Play 14***).
- □ **Identify and disseminate** lessons learned to inform and improve fraud risk management activities.

*For example, if through these efforts you identify multiple incidents of the same fraud scheme, you should communicate the details with relevant parties to ensure processes and controls are improved moving forward. Or lessons learned may require updates to training (see **Play 10**) to incorporate and disseminate this information to relevant parties.*

- □ **Coordinate** with your IG to determine what information and support documentation they need to initiate an investigation and how that information should be shared.

Play 16 - Check Your Progress

- □ **Determine** the type of monitoring and evaluation activities you would like to implement. You should consider the following recommendations:
  - This should include a mix of ongoing monitoring and separate evaluations of more targeted areas.
  - This should be comprehensive and cover the different components of your antifraud program, including awareness and training initiatives (see ***Play 3*** and ***Play 10***), fraud risk assessments (see ***Play 6)***, an analytics (see ***Play 8*** and ***Play 9***).
- □ **Use** existing monitoring activities, such as your agency's annual OMB Circular A-123 testing process to reduce burden on agency staff and streamline monitoring and reporting across program integrity functions (see ***Play 7***).
- □ **Set** the scope and frequency of monitoring and evaluation activities.

For example, if you plan to conduct targeted evaluations of your training initiatives, you may decide that this should occur ad-hoc (frequency) after each occurrence of a new training program or topic (scope). This would allow you to evaluate the effectiveness of new training programs or materials and implement lessons learned based on the results of the post-training evaluation.

*Note: As stated in bullet number 2 in **'Key Points'**, you should consider changes in the agency, its operating environment, and its control structure to determine the appropriate scope and frequency of your fraud monitoring and evaluation activities. For example, if a particular program undergoes a significant reorganization that would impact antifraud activities or risks, you may need to conduct additional evaluations until the dust settles.*

Play 16 - Check Your Progress (continued)

- ☐ **Establish** appropriate measurement criteria to assist in the monitoring and evaluation of fraud risk management activities.

  *Note: This should focus on measuring the outcomes of fraud risk management activities vs. simply reviewing the outputs of those activities. See bullet number three under **'Key Points'** for further details.*

- ☐ **Evaluate** the results of monitoring and evaluation activities against your established measurement criteria.

  *Note: See bullet number three under **'Key Points'** for further details.*

- ☐ **Remediate** deficiencies identified based on the results of monitoring and evaluation activities.

  For example, if you identify weaknesses in your internal controls related to identity verification in call centers, work with relevant program office staff to identify and mitigate the root cause and perform validation testing to verify the newly designed controls are operating effectively.

- ☐ **Communicate** the results of monitoring and evaluation activates to relevant stakeholders.

  Note: The results of your monitoring and evaluation activities should be summarized and reported to relevant agency stakeholders. This may include both senior leadership and staff aligned to the program or business function related to the area of focus of the results. For example, if you are monitoring the fraud risk assessment process of the payroll function, you should communicate the results to both relevant senior leaders and payroll-specific personnel, including the relevant payroll system owners and human resources personnel if the issues relate to the handoff between human resources and payroll functions.

Appendix C

Other Resource Repository

The playbook is not intended to be all inclusive, and is not the only resource available. We have identified additional external and intergovernmental sources that provide additional valuable information on fraud awareness, prevention and detection activities, and related best practices that can help provide further guidance when developing, implementing, or advancing your antifraud programs. See the links below for detailed information, broken out by organization.

- **Association of Certified Fraud Examiners (ACFE)**
    - **Fraud Resource Library:** The ACFE Fraud Resources Library is your source for timely and relevant antifraud information, tools, services and other resources. It offers a comprehensive collection of antifraud publications, articles and reports, sample documents, tools, videos and podcasts to support professionals with the information needed to fight fraud effectively.

      Link: http://www.acfe.com/resource-library.aspx
    - The **2018 Report to the Nations on Occupational Fraud and Abuse**: The 2018 Report to the Nations on Occupational Fraud and Abuse provides an analysis of 2,690 cases of occupational fraud that were investigated between January 2016 and October 2017. All information was provided by the Certified Fraud Examiners (CFEs) who investigated those cases. The fraud cases in this study came from 125 countries throughout the world—providing a truly global view into the plague of occupational fraud. It will help you:
        - Learn how fraud is committed and the most effective ways to detect it. Identify fraud losses at global, industry and organizational levels. Discover how organizations respond when occupational fraud has been identified.
        - Compare your organization's fraud risks by industry, region and size. Benchmark your antifraud efforts against similar organizations and against the most effective methods for reducing fraud losses.
        - See which employees or departments present the greatest fraud risk for your organization. Learn where the largest frauds are likely to occur. Identify behavioral clues that can be indicators of fraudulent conduct.

          Link: https://www.acfe.com/report-to-the-nations/2018/

- **Association of Government Accountants (AGA)**
  - **Fraud Prevention Tool:** AGA's Fraud Prevention Tool provides resources for federal, state, local and tribal government financial managers to use in preventing and detecting fraud.

    Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention.aspx
  - **Internal Controls Tool:** The Internal Controls Tool is designed to help you develop and maintain the most effective internal controls for your organization. Internal control is a process implemented by management that is designed to provide reasonable assurance regarding the achievement of objectives.

    Link: https://www.agacgfm.org/Tools-Resources/intergov/Internal-Controls.aspx

- **Other Resources**
  - **Department of Defense Office of Inspector General (OIG)**
    - **Fraud Detection Resources:** Resources on this page include general fraud schemes, indicators, red flags, and contract specific antifraud items.

      Link: http://www.dodig.mil/Resources/Fraud-Detection-Resources/
  - **Managing the Business Risk of Fraud: A Practical Guide:** This guide provides credible guidance from leading professional organizations that defines principles and theories for fraud risk management and describes how organizations of various sizes and types can establish their own fraud risk management program.

    Link: https://www.acfe.com/uploadedfiles/acfe_website/content/documents/managing-business-risk.pdf
  - **Federal Bureau of Investigations (FBI)**
    - **Common Fraud Schemes:** The following are some of the most common scams that the FBI encounters, as well as tips to help prevent you prevent them.

      Link: https://www.fbi.gov/scams-and-safety/common-fraud-schemes
    - **White-Collar Crime:** The following are some of the most common white-collar crime fraud schemes that the FBI encounters, as well as tips to help prevent you them.

      Link: https://www.fbi.gov/investigate/white-collar-crime

- **Federal Bureau of Investigations (FBI) (continued)**
  - **Cyber Crime:** The following are some of the most common cyber crime fraud schemes that the FBI encounters, as well as tips to help prevent you them.

    Link: https://www.fbi.gov/investigate/cyber

- **Grants.Gov**
  - **Grant Fraud:** Every year, hundreds of billions of dollars are distributed in the form of federal grants to universities, local governments, organizations and individuals. The vast majority of these funds are spent as intended, but misuse, deceit and abuse are nonetheless present. As a result, hundreds of thousand dollars go to waste. Learn how you can help to stop fraudulent behavior and, thus, strengthen the integrity of the federal grant system and increase the overall efficiency of the government.

    Link: https://www.grants.gov/web/grants/learn-grants/grant-fraud.html

Appendix D

Resource & Link Respository

The playbook is not intended to be allinclusive, and is not the only resource available. We have identified additional external and intergovernmental sources that provide additional valuable information on fraud awareness, prevention and detection activities, and related best practices that can help provide further guidance when developing, implementing, or advancing your antifraud programs. See the links below, broken out by play.

The Plays

Create a Culture

1. How Exposed Are You?
2. Know Where You Are and Where You Want to Be
3. Fraud is Not a Four-Letter Word
4. Create the Antifraud Dream Team

Identify and Assess

5. Think Like a Fraudster
6. Discover What You Don't Know

Prevent and Detect

7. Build on What You Have
8. Look for Quick Wins When Starting Fraud Analytics
9. Stay a Step Ahead
10. Train Your People
11. Know Thyself (and Thy Agency)
12. Sharing is Caring
13. Take What is Theirs and Make It Yours!
14. Establish a Feedback Loop with Your IG

Insight into Action

15. Take Action
16. Check Your Progress

CREATE A CULTURE

Play 1 - How Exposed are You?

There are no external or intergovernmental sources referenced in this play.

Play 2 - Know Where You are and Where You Want to Be

There are no external or intergovernmental sources referenced in this play.

Play 3 - Fraud Is Not a Four-Letter Word

- **Reference 1: Fraudweek Resource**
  - Link: http://www.fraudweek.com/what-you-can-do.aspx
  - Location: *Click here* to be navigated to the location of this reference.

Play 4 - Create the Antifraud Dream Team

- **Reference 1: ACFE's Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse**
  - Link: https://www.acfe.com/report-to-the-nations/2018/
  - Location: *Click here* to be navigated to the location of this reference.

IDENTIFY AND ASSESS

Play 5 - Think Like a Fraudster

- **Reference 2: The Fraud Triangle**
  - Link: http://www.acfe.com/fraud-triangle.aspx
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 3: ACFE Fraud Tree**
  - Link: http://www.acfe.com/fraud-tree.aspx
  - Location: *Click here* to be navigated to the location of this reference.

Play 5 - Think Like a Fraudster (continued)

- **Reference 4: AGA's Fraud Prevention Tool**
  - Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention.aspx
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 5: AGA's Fraud Prevention Tool—Resources by Business Process**
  - Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention/Tools-by-Business-Process.aspx
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 6: AGA's Fraud Prevention Tool—Resources by Program Area**
  - Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention/Tools-by-Program-Area.aspx
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 7: AGA's Fraud Prevention Tool—Resources by Fraud Type**
  - Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention/Tools-by-Fraud-Type.aspx
  - Location: *Click here* to be navigated to the location of this reference.

Play 6 - Discover What You Don't Know

- **Reference 1: AGA Fraud Prevention Tool**
  - Link: https://www.agacgfm.org/Tools-Resources/intergov/Fraud-Prevention.aspx
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 2: AGA's Fraud Prevention Tool—Risk Modelling and Assessment**
  - Link: https://www.agacgfm.org/Intergov/Fraud-Prevention/Resources-Best-Practices/Risk-Modeling-Assessment.aspx
  - Location: *Click here* to be navigated to the location of this reference.

Play 6 - Discover What You Don't Know (continued)

- **Reference 3: GAO Fraud Risk Framework:**
  - Link: https://www.agacgfm.org/Intergov/Fraud-Prevention/Resources-Best-Practices/Risk-Modeling-Assessment.aspx
  - Location: This reference appears multiple times in this Play. *Click here* to be directed to the first reference.

- **Reference 4: GAO Green Book**
  - Link: https://www.gao.gov/assets/670/665712.pdf
  - Location: *Click here* to be navigated to the location of this reference.

PREVENT AND DETECT

Play 7 - Build on What You Have

There are no external or intergovernmental sources referenced in this play.

Play 8 - Look for Quick Wins When Starting Fraud Analytics

- **Reference 1: ACFE's Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse**
  - Link: https://www.acfe.com/report-to-the-nations/2018/
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 2: Do Not Pay Business Center**
  - Link: https://www.fiscal.treasury.gov/fsprograms/fs_donotpaybc.htm
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 3: Antifraud Data Analytics Test**
  - Link: http://www.acfe.com/fraudrisktools-tests.aspx
  - Location: *Click here* to be navigated to the location of this reference.

Play 9 - Stay a Step Ahead

There are no external or intergovernmental sources referenced in this play.

Play 10 - Train Your People

- **Reference 1: ACFE's Report to the Nations, 2018 Global Study on Occupational Fraud and Abuse**
  - Link: https://www.acfe.com/report-to-the-nations/2018/
  - Location: This reference appears multiple times in this Play. *Click here* to be directed to the first reference.

- **Reference 2: International Fraud Awareness Week—Designing an Effective Antifraud Training Program**
  - Link: http://www.fraudweek.com/uploadedFiles/Fraudweek/2016/content/fraud-training-program.pdf
  - Location: *Click here* to be navigated to the location of this reference.

Play 11 - Know Thyself (and Thy Agency)

There are no external or intergovernmental sources referenced in this play.

Play 12 - Sharing Is Caring

- **Reference 1: Oversight.gov**
  - Link: www.oversight.gov
  - Location: *Click here* to be navigated to the location of this reference.

- **Reference 2: Council of the Inspectors General on Integrity and Efficiency**
  - Link: https://www.ignet.gov/

- Location: *Click here* to be navigated to the location of this reference.

Play 13 - Take What is Theirs and Make It Yours!

There are no external or intergovernmental sources referenced in this play.

Play 14 - Establish a Feedback Loop with Your IG

- **Reference 1: Oversight.gov**
  - Link: www.oversight.gov
  - Location: *Click here* to be navigated to the location of this reference.

INSIGHT INTO ACTION

Play 15 - Take Action

There are no external or intergovernmental sources referenced in this play.

Play 16 - Check Your Progress

- **Reference 1: GAO's Fraud Risk Framework:**
  - Link: https://www.gao.gov/assets/680/671664.pdf
  - Location: This reference appears multiple times in this Play. *Click here* to be directed to the first reference.

Appendix E

Acronym List

ACCT	Assess, Coordinate, Communicate, and Train
ACFE	Association of Certified Fraud Examiners
AGA	Association of Government Accountants
CMS	Centers for Medicare and Medicaid Services
CO	Contracting Officer
COR	Contracting Officer Representative
DNP	Do Not Pay Business Center
EBT	Electronic Benefit Transfer
ERM	Enterprise Risk Management
GAO	Government Accountability Office
IG	Inspector General
IoT	Internet of things
IPERA	Improper Payments Elimination and Recovery Act
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
SOP	Standard Operation Procedure
USCIS	U.S. Citizenship and Immigration Services
VBA	Veterans Benefits Administration