OFFICE of INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

An Illustrative Guide to Developing a Fraud Risk Management Framework

June 03, 2026

Office of Audit | Office of Inspector General
U.S. Department of Housing and Urban Development

OFFICE of INSPECTOR GENERAL
UNITED STATES DEPARTMENT OF HOUSING AND URBAN DEVELOPMENT

An Illustrative Guide to Developing a Fraud Risk Management Framework

Fraud can negatively affect any government program, including those funded through the U.S. Department of Housing and Urban Development (HUD). Fraud involves obtaining something of value through willful misrepresentation. Catching fraud before it occurs requires managers to evaluate how a program can be defrauded and strategically think about if the program is managed to identify and stop fraud before it occurs.

In addition to being required by Federal rules, strategically thinking about fraud helps HUD grantees efficiently mitigate fraud and avoid staff time and reputational damage when a program is defrauded. Antifraud experts commonly refer to this as "fraud risk management" and have developed a "Framework" to guide program managers.

Fraud risk management helps to ensure program integrity by continuously and strategically mitigating both the likelihood and effects of fraud. Identifying and mitigating fraud risks before payments are made decreases the likelihood fraud will occur. Good anti-fraud efforts address the risks of fraud, or how the program might be defrauded, which is commonly called a "fraud risk". Although the occurrence of fraud in an organization indicates that there is a fraud risk, a fraud risk can still exist even if no one has yet committed fraud or has identified its occurrence. Effectively managing fraud risks helps to ensure that programs fulfill their intended purpose, funds are spent effectively, and assets are safeguarded. The fraud risk management framework can assist agencies in accomplishing these goals.

Using this Guide

This Illustrative Guide and accompanying Templates are designed to help support recipients of HUD funding to manage fraud risks in HUD-funded programs.[1] The resources are designed to help HUD-funded program managers to implement the best practices from The "Program Integrity: Antifraud Playbook[2]" designed by the U.S. Chief Financial Officers Council (CFOC) and the U.S. Department of the

[1] As administrators of Federal funds, grantees are responsible for assessing and effectively mitigating fraud risks impacting the programs it administers on behalf of the Federal Government. The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 CFR 200.303(a) state that a non-Federal entity must establish and maintain effective internal control over the Federal award and that the internal controls should align with guidance in "Standards for Internal Control in the Federal Government" issued by the Comptroller General of the United States, or the "Internal Control Integrated Framework" issued by COSO (The Committee of Sponsoring Organizations of the Treadway Commission). Both frameworks include identifying, analyzing, and responding to fraud risks.

[2] *Program Integrity: The Antifraud Playbook* is designed to provide a four phased approach to fraud risk management that is in alignment with The Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards at 2 CFR 200.303(a). It utilizes successful practices from within the federal

Treasury, Bureau of the Fiscal Service (BFS), to assist the Federal, State, and local financial management community. The Antifraud Playbook lays out four "phases" for program managers to use when strategizing and evaluating antifraud activities:

There are four phases to fraud risk management:

Create a Culture—Build a culture that is conducive to both integrity efforts and furthering antifraud measures at your agency.

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.

Prevent and Detect—Develop or strengthen antifraud controls that mitigate your highest risk areas and start or advance your fraud analytics program.

Insight into Actions—Use available information, either within your agency, or from external sources, and turn that insight into actionable tasks.

Additionally, the Antifraud Playbook uses a maturity model with four (4) progressive levels. This Guide breaks down each phase using the four maturity levels to help program managers best allocate limited resources to maturing their antifraud practices. As program managers evaluate their existing programs, they can use the maturity levels to determine what next steps are to reach the desired "goal state."

To assist entities in developing a fraud risk management framework and target the four phases of fraud risk management, we have developed a series of templates for entities to use. These templates should be tailored to your organization and were created only to provide a visual starting point of what fraud risk management activities could look like in your organization. The use of these templates does not prevent HUD OIG from fulfilling its statutory responsibilities or infringe on HUD OIG's independence in doing so. The information presented and referenced by these templates and instructions is intended to help support fraud risk-management activities, including fraud risk assessments. While these templates offer examples of fraud risks related to certain programs, these examples do not represent a comprehensive and tailored assessment of specific program risks. Thus, using these templates and referenced content does not replace completing a formal fraud risk assessment. Determinations of fraud risks and the design and implementation of appropriate fraud risk-management efforts remain the responsibility of program officials.

government and private sector which aid in approaching and developing strategies for managing and combatting the risk of fraud.

Create a Culture Illustrative Guide

Fraud Risk Exposure

Calculating fraud risk exposure involves taking a high-level look at how your organization is exposed to fraud and determining where your organization should focus its efforts. To complete this template, perform the following:

1. Break your organization into components (for example: programs, activities, divisions) that make sense to your organization's operations.
2. Identify quantitative (monetary) and qualitative (non-monetary) factors that increase the risk of fraud. Use brainstorming techniques to identify these factors: Conduct workshops, interviews, or focus groups with stakeholders to brainstorm factors based on the fraud triangle (incentives/pressures, opportunities, rationalization) and other contextual elements. We have provided a few examples of these factors in the template, but there are many other factors that should be considered depending on your entity. In general, programs are more susceptible to fraud when many people are involved, controls over those people are limited, and those people or their associates can benefit from acting fraudulently.
    a. Examples of Quantitative Factors:
        i. **Financial Metrics:** High-value transactions, revenue or expense concentration in certain programs or activities, or frequent manual journal entries.
        ii. **Transaction Data:** Volume of transactions or outlays, percentage of unverified payments, or frequency of overrides in approval processes.
        iii. **Control Metrics:** Rate of control failures (e.g., 5% of reconciliations with discrepancies), number of segregation-of-duties violations, or audit findings per period.
        iv. **Operational Metrics:** Employee turnover rates, number of employees with excessive system access, or frequency of policy violations.
        v. **External Metrics:** Industry fraud loss benchmarks (e.g., 5% of revenue lost to fraud annually, per industry standard report), or number of regulatory fines.
    b. Examples of Qualitative Factors:
        i. **Incentives/Pressures:** Financial stress, performance-based bonuses, or unrealistic targets.
        ii. **Opportunities:** Weak or manual internal controls, lack of segregation of duties, decentralized processes, reliance on external parties without adequate oversight, or complex IT systems.
        iii. **Attitudes/Rationalizations:** Poor ethical tone, employee dissatisfaction, or justification of unethical behavior.
        iv. **Other Factors:** High staff turnover, inadequate training, or external pressures like economic downturns.

3. For each risk factor, rank each component of your organization. We ranked ours 1-5, with 1 being low risk and 5 being high risk; but organizations should pick a scoring system the works for them. Determining the right score for each risk factor for each organization can be subjective, but establishing objective criteria for each of the risk scores (ex. 1-5) for each factor can help to ensure objective results. See our 2 examples in the worksheet for the quantitative factors. Here are some examples of methods that can be used for objective ratings:
    a. Scoring Systems: Numeric scores for objective comparison.
        i. Qualitative Example: To assess the factor "poor ethical tone from leadership" the team may obtain employee feedback through anonymous surveys and give ratings based on a predetermined scoring system for each question.
    b. Comparative Analysis/Heat Maps: Visual tools to highlight top risks in programs.
        i. Qualitative Example: To assess the "extent of manual processes" the entity may use a comparative analysis/heat map to determine the number of manual processes across different parts of its organization. Manual process rankings should be based on the extent of manual processes identified in the heat map.
    c. Expert Consensus: Vote or discuss in workshops to finalize rankings.
        i. Quantitative Example: To assess what volume of transactions would be considered "high transaction volumes," the team could use discussions and voting. After discussion, participants vote on the range of transactions that should be associated with each ranking.
        ii. Qualitative Example: To assess the factor "incentive to commit fraud" the organization could debate it in a workshop. Some team members may believe incentive is high in one program, while others do not. Both teams present their arguments, and an independent group votes on the rating.
    d. Benchmarking: Compare against industry standards or past assessments.
        i. Quantitative Example: The entity compares "fraud-related losses" (e.g., $60,000 last year) to an Association of Certified Fraud Examiners (ACFE) industry benchmark of 5% of revenue (e.g., $50,000 for a $1M revenue firm). The above-average loss in a program elevates its ranking for this risk factor.
        ii. Qualitative Example: The program's "internal control culture" is benchmarked against industry standards (e.g., COSO framework requiring robust anti-fraud policies). The organization's lack of a formal anti-fraud program, unlike peers, means the program should be rated higher for this factor.

4. In the fraud exposure column for each component, add all the points and divide the total by the number of factors. You may also weigh certain factors higher or lower depending on your organization's environment. In the template, we provided an example for 4 programs and showed how the scores would look weighted and unweighted. If you use weighting, instead of adding all the scores up and dividing by the total number of factors, multiple each score by its weight and add up all the totals.

    Factors are weighted based on their importance to the organization's goals, risk appetite, or potential impact (e.g., financial loss, reputation). Higher weight means that the factor indicates

a greater risk of fraud than a factor with a lower weight. For example, in the template, we weighed "% of total outlays" higher than the others due to the risk of high financial impact in programs with high outlays. We also weighted “ethical tone” higher than the other qualitative factors because it enables widespread fraud. While we weighed the other qualitative factors less, the overall qualitative factors represent 70% of the total score and therefore indicate that the organization considers them very important in relation to quantitative factors.

How to Adjust Weights in Calculations:

Set Initial Weights:

i. Based on impact (financial, reputational), organizational priorities, or industry benchmarks (e.g., ACFE’s 5% revenue loss).

Adjust Weights:

i. Triggers: New data (e.g., audit findings), regulations, or stakeholder input.

Process: Reassess in workshops, compare to benchmarks, recalculate scores.

After completing this template, your organization will have a high-level view of how it is exposed to fraud in the different components and where to start/focus fraud risk efforts. This can help to inform your enterprise wide- strategy, as higher risk components should be prioritized. See Appendix A.

Determine Your Goal State

In the Goal State template, describe where you are and your goal. Below are definitions of each level based on The CFO Antifraud Playbook:

1. Ad Hoc – Fraud risk management processes are disorganized, even chaotic, and antifraud efforts are undocumented and in a state of dynamic change, tending to be driven in an ad hoc, uncontrolled, and reactive manner. This is not a goal state for agencies with fraud exposure.

2. Initial – The agency is aware of the need for a more formal fraud risk management approach, and repeatable processes have been developed. Risks are still managed largely in a reactive way.

3. Operational – Fraud risk management activities across the organization are aligned with controls, and information on fraud risks is aggregated and analyzed and is easily available to the necessary individuals. The goal state for agencies with low fraud risk exposure is an initial to operational maturity level.

4. Leadership – The agency’s focus is on continually improving fraud risk management through both incremental and innovative changes or improvements. Risks are managed largely in a proactive way. The goal state for agencies with high fraud exposure is an operational to leadership maturity level.

This template should be used to think about where your organization is and where your organization wants to go, which should inform your entity wide strategy. Using this template will help your organization determine how its current activities rank on the maturity scale and to set goals for

improvement. Under the Current State of Activities, describe your entity in each phase assesses and determine the maturity level/description that best matches your organization for each phase (phases are listed in each column). Then, use the goal state activities section of the template to set goals and describe where you want to go and how you want to improve in each phase. In the set of columns, list actional steps that your organization plans to take to reach its goal state. Your organization should consider other activities outlined in the next template (Enterprise-wide strategy) when determining the actionable steps it should take. See Appendix B.

Enterprise-wide Strategy

An enterprise-wide strategy is critical to outline how your agency will identify, prevent, and detect fraud. This strategy should be distributed to the entire agency so that everyone understands their role. This template assists in outlining the strategy the organization will use to cover the 4 phases of fraud risk management previously discussed above: Create a Culture, Identify and Assess, Prevent and Detect, and Insight into Actions. In this template, examples have been provided as to what should be addressed in an enterprise-wide strategy. Most significantly, this strategy should include information on the following key components:

Governance and Leadership: Clear information on who is leading this effort. This should be a dedicated team overseeing fraud risk management, including the development and execution of policies and procedures. There should be a strong tone of support from top management as well as a budget and resources to execute the necessary processes.

Risk Assessments: The organization's process for risk identification through regular brainstorming and evaluation of fraud risks across the organization.

Internal Controls: The organization's process to align internal controls to address fraud risks that are identified in the risk assessment.

Data Analytics/Technology/Tools: The organization's data analytics strategy. If possible, leverage the latest technology to implement advanced antifraud analytics tools such as AI and data analytics to detect anomalies and patterns indicative of fraud. If this is not possible for your organization at this time, start with the data and tools you have and set future goals. Advanced technology can analyze transactions and other risk factors which will allow organizations to flag suspicious activities before they result in irreparable harm to the organization

Monitoring Effectiveness of Antifraud Activities: The organization's plan to continually improve its antifraud program. The organization should utilize monitoring and metrics to determine how well current anti-fraud activities are working, and report on effectiveness to leadership. See Appendix C.

Fraud Risk Team

For successful implementation of your enterprise-wide strategy to reach your goal state, establishing an antifraud tone throughout your organization is critical. To achieve this, it is important to designate a specific group of people in your organization with oversight of fraud risk management, including members of senior management. When utilizing this template, the most important step that you will need to accomplish is to take the time to understand the roles and responsibilities that personnel at all levels of the organization will have with respect to fraud risk management.

All levels of staff, including management, should: 1) Have a basic understanding of fraud and be aware of the red flags, 2) Understand their role in fraud risk management, 3) Understand how their job procedures are designed to manage fraud risks and when noncompliance may create an opportunity for fraud to occur or go undetected, 4) Read and understand policies and procedures (e.g. the fraud policy, code of conduct, and whistleblower policy), as well as other operational policies and procedures, such as procurement manuals.

While strong controls against fraud are the responsibility of everyone in the organization, the fraud risk team leads fraud risk management activities. This template includes just a few examples and information on various roles that are important in a fraud risk management program but is not all inclusive. See Appendix D.

Fraud Risk Team- Mission Statement

It is important that the team dedicated to fraud risk understands its mission. This will allow the team to have a clear focus when making decisions while evaluating and mitigating risks. Therefore, this template provides an example of what the mission statement may look like for a group that is designated to develop and implement fraud risk management for its organization. See Appendix E.

Code of Conduct

Ensuring all employees are accountable and aware of their expectations responsibilities in fraud risk management is critical to successful fraud risk management. In this template we have included an example of a code of conduct that could be used to outline the core principles all employees and contractors should abide by, as well as other responsibilities and prohibited activities that employees and contractors need to be aware of. See Appendix F.

Promoting Fraud Awareness

Promoting fraud awareness is important because members of your organization may not understand how your entity is exposed to fraud and may believe that fraud does not exist. The Fraud Risk Team should brainstorm to come up with ways to promote fraud awareness within your organization. This should include a clear method for personnel to report fraud as it is critical that everyone in your organization knows how to report fraud in order to have effective fraud risk management. In this

template, we have included examples of activities that can be used to promote fraud awareness including creating a fraud hotline or website for reporting fraud. See Appendix G.

Identify and Assess Illustrative Guide

Fraud Risk Inventory

A fraud scheme is a specific scenario where fraud could occur within the organization's processes, systems, or relationships. Before conducting a risk assessment, it is important to identify all potential fraud schemes in a fraud risk inventory. A fraud risk inventory identifies all of ways that your organization could be vulnerable. When creating the fraud risk inventory, you will need to think like a fraudster while developing the list. In this template, you should brainstorm schemes that can impact all components of our organization (program/division, and activities). To complete this, you may need to perform the following:

i. Conduct workshops or interviews with key stakeholders (e.g. finance, procurement, IT) to brainstorm potential fraud scenarios.
ii. Review historical fraud incidents, audit findings, and industry reports to identify common fraud schemes.

The inventory should be done for each component in your organization. You will need to document each scenario with a clear description (e.g. "An employee submits falsified expense reports to receive unauthorized reimbursements").

Example Scenario: "Vendor collusion with an employee to inflate invoices for kickbacks."

In the template, the actor is who could commit this fraud scheme, and the fraud risk entry point is where in the process it could occur.

When creating your fraud risk inventories, we suggest that you see the HUD OIG audit report on potential fraud schemes (2022-FO-0007.pdf) for examples of fraud schemes as well as the GAO Antifraud Resource (https://antifraud.gaoinnovations.gov/resources). In the template we provided a few examples, but each entity is different and should list many more schemes. The fraud schemes in red were carried through to the fraud risk assessment and fraud risk profile tabs as an example of how to use the fraud risk inventory to create a fraud risk assessment and fraud risk profile. See Appendix H.

Fraud Risk Assessment

Fraud risk assessments should be performed for each component (program/activity) across the organization and tailored to that program/activity. Conducting a risk assessment involves identifying and using the fraud schemes from the fraud risk inventory, assessing the likelihood of occurrence and impact, and evaluating the effectiveness of mitigating controls. This process quantifies the organization's exposure to fraud risks before and after controls prioritizing risk management efforts and allocate resources efficiently.

In this template, we provide an example of what a fraud risk assessment could look like for Program #1 (from the Fraud Risk Inventory template above). Perform the following to complete this template-

1) **Fraud Schemes**- carry over the listing from the fraud risk inventory to complete column 1.
2) **Identify Fraud Risk Factors** - Fraud risk factors are conditions or vulnerabilities that increase the likelihood or impact of a fraud scenario, such as weak controls, opportunity, or motivation.
   i. Analyze each fraud risk scheme to identify contributing factors using the fraud triangle (opportunity, pressure, rationalization).
      a. Opportunity: Weak segregation of duties, lack of oversight.
      b. Pressure: Financial distress, performance incentives.
      c. Rationalization: Perceived unfair treatment, lax ethical culture.
   ii. Consider external factors (e.g. economic conditions, regulatory changes) and internal factors (e.g. system vulnerabilities, employee turnover).
   iii. Document specific risk factors for each scenario.
   Example: For vendor collusion scheme:

      a. Opportunity: Single employee approves vendor invoices without review (lack of segregation of duties).
      b. Pressure: Employee faces personal financial difficulties.
      c. Rationalization: Belief that "everyone does it" due to weak ethical tone.

3) **Assess Inherent Likelihood (Before Controls)**- Inherent likelihood is the probability of a fraud scenario occurring without any mitigating controls in place and is expressed on a standardized scale.
   i. Define a likelihood scale (e.g. 1–5, where 1 = Rare, 2 = Unlikely, 3 = Possible, 4 = Likely, 5 = Almost Certain).
   ii. Evaluate each scenario based on fraud risk factors and historical data (e.g. frequency of similar incidents in the organization or industry).
   iii. Assign a numerical score to each scenario and document the rationale.
   Example: For falsified tenant eligibility (scheme 1 in the template), assign a score of 4 (Likely) due to weak oversight and high vendor transaction volume.

   Formula: Inherent Likelihood Score = Assigned score (1–5).

4) **Estimate Quantitative Impact (Financial Loss)**- Quantitative impact is the estimated financial loss if the fraud scheme occurs, measured in monetary terms.
   i. Estimate the direct financial loss for each scenario (e.g. stolen funds, overpaid rents/invoices).
      a. Use historical data, average transaction values, or industry benchmarks.
      b. Consider worst-case, most likely, and best-case loss scenarios.
   ii. Include indirect costs where feasible (e.g. legal fees, reputational damage, operational disruptions).
   iii. Calculate the expected financial loss as a single value (e.g. most likely loss or an average of scenarios).

iv. Document assumptions and sources for transparency.
Example:

Direct loss: $50,000 (inflated invoices over 6 months).

Indirect loss: $10,000 (investigation costs).

Total Quantitative Impact = $60,000.

Formula: Quantitative Impact = Direct Loss + Indirect Loss (if applicable).

5) **Calculate Total Quantitative Exposure (Before Controls)**- Total quantitative exposure (before controls) is the expected financial loss from a fraud scheme, factoring in its inherent likelihood and quantitative impact.
   i. Convert the inherent likelihood score (1–5) to a probability percentage based on the scale (e.g. 1 = 10%, 2 = 30%, 3 = 50%, 4 = 70%, 5 = 90%).
   ii. Multiply the quantitative impact by the probability to calculate the expected exposure.
   iii. Document the result for each scenario.
   Example:

   Inherent Likelihood = 4 (70% probability).

   Quantitative Impact = $60,000.

   Total Quantitative Exposure (Before Controls) = $60,000 × 0.7 = $42,000.

   Formula: Total Quantitative Exposure (Before Controls) = Quantitative Impact × Inherent Likelihood Probability.

Identify and Evaluate Mitigating Controls- Mitigating controls are preventive measures that reduce the likelihood or impact of a fraud scenario.

i. Map existing controls to each fraud risk scenario (e.g. segregation of duties, automated transaction monitoring).
ii. Evaluate the effectiveness of each control based on design and implementation (e.g. strong, moderate, weak).
   a. Strong: Fully addresses the risk
   b. Moderate: Partially addresses the risk
   c. Weak: Minimal impact

Assess Likelihood of Occurrence (After Controls)- Likelihood of occurrence (after controls) is the revised probability of a fraud scenario occurring after factoring in the effectiveness of existing mitigating controls.

i. Reassess the likelihood score (1–5) for each scenario, considering the strength of mitigating controls.
ii. Adjust the score downward based on control effectiveness (e.g. strong controls may reduce likelihood by 2 levels).
iii. Document the revised score and rationale.

Formula: Likelihood of Occurrence (After Controls) = Revised score (1–5).

Calculate Total Quantitative Exposure (After Controls)- Total quantitative exposure (after controls) is the expected financial loss after accounting for the reduced likelihood due to mitigating controls.

i. Convert the revised likelihood score (after controls) to a probability percentage (e.g. 1 = 10%, 2 = 30%, 3 = 50%, 4 = 70%, 5 = 90%).
ii. Multiply the quantitative impact by the revised probability to calculate the residual exposure.
iii. Document the result for each scenario.
Example:

Likelihood of Occurrence (After Controls) = 2 (30% probability).

Quantitative Impact = $60,000.

Total Quantitative Exposure (After Controls) = $60,000 × 0.3 = $18,000.

Formula: Total Quantitative Exposure (After Controls) = Quantitative Impact × Likelihood of Occurrence Probability (After Controls). See Appendix I.

Fraud Risk Profile

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 of occurrence and impact, risk tolerance, risk prioritization, response activity, and owner (CFO Antifraud playbook). In this template, we included 2 examples of high priority fraud schemes, but the organization will likely have more.

- Likelihood and Impact- use the information from the fraud risk assessment to determine likelihood and impact
- Risk Tolerance- management's willingness to accept the risks associated with fraud
- Risk Prioritization- How significant is the fraud risk based on an analysis of the likelihood and impact, as well as the effectiveness of existing controls?
- Response Activity- What actions does the program plan take to address the fraud risk, if any, in order to bring fraud risks within managers' risk tolerance? Information in this row relates to the antifraud strategy and the specific actions managers decide to take to avoid, share, accept, or reduce fraud risks.
- Owner- Which group or individual within the program is responsible for addressing the risk? The owner of the fraud risk will vary by program, but generally, this is the entity with accountability for addressing the fraud risk. See Appendix J.

Definitions from GAO-15-593SP, A Framework for Managing Fraud Risks in Federal Programs

Repeat and Expand Fraud Risk Assessments

Fraud risk assessments should occur regularly and expand as the organizations fraud risk management program matures. You should be able to repeat the steps we previously provided above for developing and implementing your organization's fraud risk assessments. In this template we have outlined several actions involved in this process and examples of the frequency and outcomes expected. See Appendix K.

Prevent and Detect Illustrative Guide

Implementing/Refining Control Activities

Using the risk assessment results, design and implement specific controls activities, including policies, procedures, techniques, mechanisms and feedback loops to prevent and detect fraud. When implementing control activities, keep in mind that data sharing and data analytics programs can be a great way for organizations to efficiently identify fraud. The template provides examples of control activities for different risk areas.

To implement effective controls your organization will need to document and assess current controls to mitigate fraud risks, identify gaps in current controls, and identify/implement additional controls or improvements. See example below-

i. Document the controls and their assessed effectiveness.
Example:

Control 1: Require dual approval for invoices over $5,000.

Control 2: Monthly vendor payment audits.

ii. Identify gaps and propose additional controls if needed during this process.

From example above:
Gap: Manual processes are involved in Control 1 and collusion could occur.
Proposed additional control from example above: Use data analytics to identify anomalies in invoice pattern or amounts. If possible, implement automated invoice verification software. See Appendix L.

Insight into Action Illustrative Guide

Consistently Acting on Potential Fraud and Changing Processes to Mitigate Exploited Fraud

When fraud risk is identified from control activities or other means, consistently acting on it is a very important part of fraud risk management. This includes maintaining a working list of potential fraud identified and how they were handled, specific procedures on how to identify and what to do with potential fraud and adjusting processes procedures to respond to identified fraud. The template provides several steps that should be considered once potential fraud is identified. See Appendix M.

Measuring the Effectiveness of Detection and Prevention Activities

Since the world is constantly changing, it is very important to continuously measure the effectiveness of fraud risk management activities. The template provides several evaluation processes that can be used to evaluate the effectiveness of polies, prevention activities, detection activities, monitoring processes, and the fraud risk management program as a whole. See Appendix N.

Appendixes

Appendix A – Fraud Risk Exposure

Components	Quantitative Factors		Qualitative Factors						Fraud Exposure	
	Transaction Data	**Control Metrics**	**Opportunities**				**Incentive**	**Attitudes /Rationalization**		
	% of total outlays	Rate of controls failures	Are duties adequately segregated?	How reliant is the entity on outside parties to perform controls/perform verification?	How prevalent are manual processes?	How decentralized are processes?	Is there an incentive to commit fraud (i.e., there is something to gain from committing fraud)?	Is the current ethical tone weak? Are employees dissatisfied?		
Weights	20%	10%	10%	10%	10%	10%	10%	20%	100%	
Program 1 Unweighted	5	2	3	4	4	3	3	2	3.3	Medium-high
Program 1 Weighted	1.0	0.2	0.3	0.4	0.4	0.3	0.3	0.4	3.3	Medium-high
Program 2 Unweighted	4	2	1	5	5	4	2	3	3.3	Medium
Program 2 Weighed	0.8	0.2	0.1	0.5	0.5	0.4	0.2	0.6	3.3	Medium-high
Program 3 Unweighted	2	3	3	3	1	2	3	3	2.5	Medium
Program 3 Weighted	0.4	0.3	0.3	0.3	0.1	0.2	0.3	0.6	2.5	Medium
Program 4 Unweighted	2	1	2	1	1	2	2	3	1.8	Low-Medium
Program 4 Weighted	0.4	0.1	0.2	0.1	0.1	0.2	0.2	0.6	1.9	Low-Medium

Ratings for Quantitative Risk Factors

Example Rankings for % of total outlays		Example Rankings for Rate of Control Failures	
Risk level	**% of total outlays**	**Risk level**	**Control Failures**
5- High risk	More thenthan 50%	5- High risk	Internal and external audits/reviews found pervasive internal control failures or management isare not addressing smaller but significant control failures
4- Medium-High	21-49%	4- Medium-High	Internal and external audits/reviews found more than 4 significant control failures that management is working to address
3- Medium risk	11-20%	3- Medium risk	Internal and external audits/reviews found 1-4 significant control failures that management is working to address
2- Low-medium	6-10%	2- Low-medium	Internal and external audits/reviews found 1-5 minor control failures that have been addressed
1- Low risk	1-5%	1- Low risk	Internal and external audits/reviews found 0 control failures or minor failures were found and addressed

Example Rankings for Fraud Exposure

Risk level
4.1- 5- High risk
3.1-4- Medium-High
2.1-3- Medium risk
1.1- 2- Low-medium
0-1- Low risk

Appendix B – Goal State

OUR CURRENT STATE OF ACTIVITIES:

(Determine the maturity level for each column that best represents your organization for each phase.)

Create a Culture	Identify and Assess	Prevent and Detect	Insight into Action

GOAL STATE

Create a Culture	Identify and Assess	Prevent and Detect	Insight into Action

ACTIONABLE STEPS TO BE EXECUTED:

(Determine the maturity level for each column that best represents your organization for each phase.)

Create a Culture	Identify and Assess	Prevent and Detect	Insight into Action

Appendix C – Enterprise-Wide Strategy

EXAMPLE ACTIVITIES: CREATE A CULTURE

Governance & Leadership	Policies & Procedures	Culture/Tone of Integrity	Budget & Resources
Anti-Fraud Governing Body: Establish function to oversee the strategy/activities. Should include Sr./Exec Leadership Oversee Policy Development, Resource Allocation and monitoring progress	**Code of Conduct:** Develop and enforce a code of conduct that emphasizes ethical behavior and zero tolerance for fraud.	**Tone at the Top:** Ensure leadership demonstrates a commitment to ethical behavior and fraud prevention.	**Resource Allocation:** Allocate sufficient budget and resources for technology, training, and personnel.
Roles and Responsibilities: Define roles of employees, managers, and execs around fraudaround fraud prevention and detection.	**Fraud Prevention Policy:** Outline specific measures to prevent fraud, including segregation of duties, authorization controls, and access restrictions.	**Recognition and Rewards:** Recognize employees who contribute to fraud prevention efforts.	**ROI Analysis:** Measure the return on investment for anti-fraud initiatives.
	Whistleblower Program: Establish a secure and anonymous reporting mechanism for employees to report suspicious activities.	**Zero Tolerance:** Enforce strict consequences for fraudulent activities.	

Governance & Leadership	Policies & Procedures	Culture/Tone of Integrity	Budget & Resources
	Incident Response Plan: Define steps for responding to and investigating fraud incidents.	**Employee Responsibilities:** To act with integrity, honesty, and transparency in all their duties. To be role models/stewards of the ethical culture the organization promotes through its leaders.	

EXAMPLE ACTIVITIES: IDENTIFY AND ASSESS

Risk Assessment
Fraud Risk Identification: Conduct a thorough assessment to identify potential fraud risks across all business units and processes of the entity.
Risk Prioritization: Rank risks based on likelihood and impact.
Ongoing Monitoring: Implement a process for continuous risk assessment and updates.

EXAMPLE ACTIVITIES: PREVENT AND DETECT

Training & Awareness	Internal Controls	Data Analytics/Technology & Tools	Investigation & Response
Employee Training: Conduct regular training sessions to educate employees on fraud risks, prevention techniques, and reporting procedures.	**Segregation of Duties:** Ensure no single individual has control over all aspects of any critical transaction.	**Fraud Detection Systems:** Implement advanced antifraud analytics tools such as AI, machine learning, and data analytics to detect anomalies and patterns indicative of fraud.	**Investigation Team:** Establish a dedicated team to investigate fraud allegations.
Leadership Training: Train managers and executives onin recognizing red flags and fostering a culture of integrity.	**Approval Processes:** Implement multi-level approval processes for high-risk transactions.	**Automated Monitoring:** Use real-time monitoring systems for transactions, employee activities, and vendor interactions.	**Forensic Capabilities:** Equip the team with forensic tools and expertise to conduct thorough investigations.
Awareness Campaigns: Use internal communications to reinforce the importance of fraud prevention.	**Regular Audits:** Conduct internal and external audits to assess the effectiveness of controls.	**Data Security:** Strengthen cybersecurity measures to prevent data breaches and unauthorized access.	**Corrective Actions:** Implement corrective measures to address vulnerabilities identified during investigations.
	Vendor and Third-Party Due Diligence: Screen vendors and partners for potential fraud risks.	**Audit Trails:** Maintain logs/ documentation of all transactions and system activities.	**Legal and Regulatory Compliance:** Where applicable report to appropriate legal/regulatory bodies such as the OIG and/or Agency and/or DOJ.

EXAMPLE ACTIVITIES: INSIGHT INTO ACTION

Regulatory & Legal Compliance	Monitoring & Reporting	Review Update & Adjust
Compliance Framework: Align the strategy with relevant laws, regulations, and industry standards	**Performance Indicators:** Define metrics to measure the effectiveness of the anti-fraud strategy (e.g., number of incidents detected, time to resolve cases, financial losses prevented).	**Annual Review:** Conduct an annual review of the strategy to ensure it remains effective and relevant.
Reporting Obligations: Ensure timely reporting of fraud incidents to regulatory authorities, if required.	**Regular Reporting:** Provide periodic reports to the steering committee and board of directors.	**Adaptation:** Update the strategy to address emerging fraud risks and technological advancements.
	Continuous Improvement: Use feedback and data to refine and enhance the strategy.	

Appendix D – Fraud Risk Team

Role	Responsibilities	Key Skills	Reports To	Interacts With	Tools and Systems	Success Metrics
Board	Be a proactive force in safeguarding the organization against fraud by 1by 1) Performing oversight responsibilities, including understanding fraud types and their impact on the entity. 2) Fostering a culture of integrity and accountability. 3) Monitor reports on fraud and oversee internal controls established by Management.	Risk and Strategy Management, Finance, Leadership and Decision-making, Industry Knowledge, Ethical Judgment and Integrity	State/Local Govt or other regulatory body.	Executive Leadership/ Senior Management	Consultants, Governance Frameworks, Risk Assessment Software, Data Analytics, Machine Learning/AI	Risk Reduction, Culture Shift, Policy Implementations, Entity wide knowledge/awarenes s improvement.
Chief Risk Officer	Develop and implement risk exposure, culture, policies and procedures, compliance, mitigation strategies and overall fraud risk management program.	Extensive experience in risk management, finance, or a related area, typically in leadership roles. Strong analytical skills and leadership	Executive Leadership	All entity component Leads	Enterprise Risk Management (ERM) Systems, Risk Assessment Software, Data Analytics Platforms	Reduction in fraud incidents, successful policy planning and strategies.

Role	Responsibilities	Key Skills	Reports To	Interacts With	Tools and Systems	Success Metrics
Program Fraud Risk Manager	Oversee all aspects of fraud risk management, strategy development, and policy implementation for specific program/component	Extensive experience in risk management, knowledge of fraud schemes, leadership skills	Chief Risk Officer	Senior Management, Team Leads	Risk assessment tools, data analytics software	Reduction in fraud incidents, successful policy implementation
Data Analyst	Analyze data to identify fraud patterns, trends, and anomalies	Strong analytical skills, proficiency in Data analytics and experience with data visualization tools	Fraud Risk Manager	IT, Operations	Data analytics platforms, BI tools like Tableau/Power BI	Number of actionable insights provided,provided accuracy of fraud prediction
Compliance Officer	Ensure all fraud prevention strategies comply with regulations and internal policies and determine if current compliance controls can be expanded to complimentcomplement fraud risk management.	Knowledge of legal and regulatory frameworks, detail-oriented	Fraud Risk Manager	Legal, HR	Compliance management software	Compliance rate, audit findings
Investigator	Investigate suspected fraud cases, gather evidence, and prepare case reports	Background in law enforcement or investigative work, analytical thinking	Fraud Risk Manager	Legal, HR, External Agencies	Case management systems, forensic tools	Case resolution rate, recovery of losses
Training Coordinator	Develop and deliver training programs on fraud awareness and prevention	Experience in training development,	Fraud Risk Manager	All employees	Learning Management Systems	Training completion rates, participant feedback

Role	Responsibilities	Key Skills	Reports To	Interacts With	Tools and Systems	Success Metrics
		good communicator				
IT Security Specialist	Implement technical measures to prevent cyber fraud, secure systems	Cybersecurity expertise, familiarity with network security tools	Fraud Risk Manager	IT Department	Security software, Security Information and Event Management (SIEM) systems	Improvement in system security posture, reduction in cyber fraud incidents, timely resolution of fraud-related customer issues
Customer Liaison	Handle customer inquiries and issues related to fraud, manage communications	Customer service experience, empathy, problem-solving skills	Fraud Risk Manager	Customer Service, Marketing	Customer Relationship Management (CRM) systems	Customer satisfaction scores
Fraud Prevention Specialist	Design and update fraud prevention measures, monitor for new fraud tactics	Knowledge of fraud mechanisms, proactive mindset	Fraud Risk Manager	Product Development, Operations	Fraud detection software	Implementation of new prevention measures, decrease in successful fraud attempts

Example Mission Statement:

At (**Entity Name**), our Fraud Risk Management Program is dedicated to safeguarding the integrity, assets, and reputation of our organization by proactively identifying, assessing, mitigating, and monitoring fraud risks. We are committed to fostering a culture of ethical behavior, transparency, and accountability, ensuring compliance with applicable laws, regulations, and industry standards. Through collaboration, innovation, and continuous improvement, we strive to protect the interests of our stakeholders, promote trust, and uphold the highest standards of governance and risk management.

Core Principles:

- Integrity: Upholding ethical standards and promoting a zero-tolerance approach to fraud.
- Act Proactively: Anticipating and addressing fraud risks before they materialize.
- Collaboration: Engaging stakeholders across the organization to build a unified defense against fraud.
- Transparency: Ensuring clear communication and reporting of fraud risks and mitigation efforts.
- Resilience: Continuously adapting to evolving fraud threats through innovation and learning.

Commitment:

We are committed to creating a secure environment where fraud risks are minimized, and any instances of fraud are promptly detected, investigated, and resolved. By embedding fraud risk management into our organizational culture, we aim to protect our resources, maintain stakeholder confidence, and contribute to the long-term success of (**Entity Name**).

Appendix F – Code of Conduct

Example Code of Conduct

1. Purpose- This Code of Conduct outlines the principles and expectations for all employees, contractors, and stakeholders to ensure a culture of integrity, transparency, and accountability. It is designed to prevent, detect, and respond to fraudulent activities that may harm the organization, its stakeholders, or its reputation.

2. Scope

This Code of Conduct applies to all employees, contractors, vendors, and third parties associated with (Entity Name). It covers all business activities, including financial transactions, reporting, and operational processes.

3. Core Principles

- Integrity: Act honestly and ethically in all business dealings.
- Transparency: Ensure all actions and decisions are open and documented.
- Accountability: Take responsibility for actions and report any suspicious activities.
- Compliance: Adhere to all applicable laws, regulations, and internal policies.

4. Prohibited Activities

The following activities are strictly prohibited and may result in disciplinary action, including termination and legal consequences:

- Fraudulent Financial Reporting: Misrepresenting financial records or reports.
- Theft or Misuse of Assets: Misusing company funds, property, or resources.
- Bribery and Corruption: Offering, accepting, or soliciting bribes or kickbacks.
- Conflict of Interest: Engaging in activities that conflict with the organization's interests.
- Falsification of Documents: Altering or fabricating records, invoices, or contracts.
- Unauthorized Disclosure: Sharing confidential or proprietary information without authorization.

5. Responsibilities

- Employees: Report any suspected fraudulent activities to the appropriate authority (e.g., Fraud Risk Management Team, Reporting Hotline).
- Managers: Foster a culture of integrity and ensure compliance with this Code of Conduct.
- Fraud Risk Management Team: Investigate reported incidents, implement controls, and provide training.
- Third Parties: Comply with this Code of Conduct and report on any unethical behavior.

6. Reporting Mechanisms
- Ethics Hotline: Report concerns anonymously via [Hotline Number/Email].
- Direct Reporting: Notify your supervisor, manager, or the Fraud Risk Management Team.
- Whistleblower Protection: Retaliation against individuals who report in good faith is strictly prohibited.

7. Training and Awareness
- All employees and contractors must complete mandatory fraud risk management training annually.
- Regular communication and updates on fraud prevention measures will be provided.

8. Investigation and Disciplinary Action
- All reported incidents will be investigated promptly and thoroughly.
- Disciplinary action will be taken against individuals found in violation of this Code of Conduct, up to and including termination and legal action.

9. Continuous Improvement
- The Fraud Risk Management Program will be reviewed and updated regularly to address emerging risks and ensure effectiveness. (only include this one for those that are involved in this process)

10. Acknowledgment

All employees and contractors are required to acknowledge receipt and understanding of this Code of Conduct by signing below:

Name: _____
Signature: _____
Date: _____

Appendix G – Promoting Fraud Awareness

Activity	Objective	Target Audience	Method	Success Metrics
Leadership Fraud Conference/Seminar/Think Tank	To empower Leadership to become a proactive force in safeguarding the organization against fraud by recognizing, preventing, and responding effectively to fraud risks within the organization.	IG, Board of Directors, Investigations	Policy Reviews, Strategy Sessions, Updates, Collaboration with Management, Resource Distribution	Knowledge Improvement, Policy Implementation, Culture Shift, Risk Reduction
Fraud Awareness Week	Increase general awareness about common fraud schemes.	All employees, customers	Workshops, seminars, and interactive sessions	Number of attendees, post-event survey feedback
Fraud Alert System	Immediate notification of new or emerging fraud tactics.	Employees, management	Email alerts, internal memos	Time from threat detection to alert distribution, feedback on alert relevance
Fraud Case Studies	Provide real-life examples to illustrate fraud methods and consequences.	New hires, all staff	Monthly presentations, case studies in training modules	Engagement in discussions, quiz scores on fraud recognition
Poster Campaign	Visual reminders in high-traffic areas to keep fraud prevention at the top of mind.	All employees, visitors	Posters in break rooms, near elevators, etc.	Observed behavior changes, feedback from staff

Activity	Objective	Target Audience	Method	Success Metrics
Internal Newsletter	Regular updates on fraud trends, prevention tips.	Employees	Email newsletter	Open rates, click-through rates to resources
Interactive Online Training	Deep dive into fraud types, prevention strategies, and company policies.	All staff	E-learning platform with quizzes and badges	Completion rates, quiz pass rates
Phishing Simulation	Educate Teach on recognizing and responding to phishing attempts.	Employees	Email simulations, follow-up training	Participation rate, decrease in click rates on phishing emails over time
Fraud Hotline or Website	Encourage reporting of suspicious activities anonymously.	All stakeholders	Dedicated phone line or web form	Number of reports, percentage of actionable tips
Customer Awareness Programs	Educate Teach customers on to protectingprotect themselves from fraud.	Customers	Information on bills, website notices, social media campaigns	Customer feedback, increase in use of security features
Fraud Prevention Workshops	Detailed sessions for departments/programs most at risk.	Finance, IT, HR	Tailored workshops with practical exercises	Participant feedback, implementation of learned strategies

Appendix H – Fraud Risk Inventory

Program / Division 1

General Fraud Category	Fraud Scheme Type	Fraud Scheme	Actor(s)	Fraud Risk Entry Point	Fraud Scheme Description
Asset Misappropriation	Fraudulent Disbursements	Falsified Tenant Eligibility	Grantee/ Subrecipient/ EmployeeSubrecipient Employee	Application or certification	Tenants or organization staff falsify income, family size, or eligibility data to qualify a tenant for vouchers.
Asset Misappropriation	Fraudulent Disbursements	Landlord Overbilling	Landlord	Expense Reimbursement	Landlords charge organization for higher rents than agreed or for vacant/unoccupied units and then pocket the extra cash.
Asset Misappropriation	Fraudulent Disbursements	Employee Timecard Fraud	Employee or contractor	Expense Reimbursement	Employee or contractor charges organization for time spent not working
Asset Misappropriation	Fraudulent Disbursements	Bribery for Maintenance Contracts	Contractor/vendor and employee	Expense Reimbursement	An employee contracts with a related party for administration, maintenance, or other services then agrees to pay inflated costs. The employee may receive kickbacks for their participation.

Program / Division 2

General Fraud Category	Fraud Scheme Type	Fraud Scheme	Actor(s)	Fraud Risk Entry Point	Fraud Scheme Description
Asset Misappropriation	Fraudulent Disbursements	Altered payee	Subrecipient, Vendor/Contractor	Contract Procurement/Payment	An employee diverts funds to their personal bank account.
Asset Misappropriation	Fraudulent Disbursements	Duplication of Benefits	Project owner	Expense Reimbursement	A project owner uses HUD funds to cover the cost of property repairs then files an insurance claim to repair the same damage and pockets the funds from the insurance claim.
Asset Misappropriation	Fraudulent Disbursements	Ghost beneficiaries	PHA employee, property management, grantee, or subrecipient	Contract Procurement	A landlord (or other actor) creates fake tenants through the use ofusing identifyidentity theft or synthetic identities to collect additional rent subsidies.
Asset Misappropriation	Bribery	False Certification/ Bribery	PHA/Grantee/Subrecipient EmployeeSubrecipient Employee	Collections	An inspector accepts bribes for favorable inspection reports and signs off on repairs that have not been completed or does not report items that do not pass inspection.
Asset Misappropriation	Fraudulent Disbursements	Mischaracterized expenses	Contractor/Beneficiary	Expense Reimbursement Program application	Deliberately using funds for ineligible purposes, such as ineligible units or loans to employees.

Activities

General Fraud Category	Fraud Scheme Type	Fraud Scheme	Actor(s)	Fraud Risk Entry Point	Fraud Scheme Description
Asset Misappropriation	Financial Statement Fraud/fraudulent disbursements	False reporting	Financial reporting staff	Data entry	Financial reporting staff hides program income that is collected and colludes with program staff that pockets the money.
Asset Misappropriation	Fraudulent disbursements	Shell Company or Organization	Subrecipient, Contractor	Procurement	An individual can set up a fraudulent organization or vendor claiming to provide services for homeless or at-risk for homeless persons to receive awards and claim funds with no intention to perform work or provide services.

Appendix I – Fraud Risk Assessment

Fraud Risk Scheme	Example Fraud Risk Factors	Inherent Likelihood (Before Controls)	Quantitative Impact (Financial Loss) ($)		Total Quantitative Impact (Financial Loss) ($)	Total Quan Exposure (Before Controls)	Examples of Existing Mitigating Controls	Effectiveness of Controls	Likeli-hoodLikelihood of (After Controls)	Total Quan Exposure (After Controls)	SAVINGS/ Exposure Reduction with existing controls $
			Direct Loss	Indirect Loss							
Falsified Tenant Eligibility	Weak income verification, high volume of transactions	4	$50,000 (lost funding/ subsidy for those eligible)	$10,000	$60,000	$42,000	Income audits, recertification	Moderate	2	$18,000	$24,000
Landlord Overbilling	Lack of rent reasonableness checks	5	$80,000 (overpayments)	$5000 (Investigation)	$85,000	$76,500	Rent comparability reviews	Moderate	4	$53,550	$22,950
Employee Timecard Fraud	Manual timekeeping, lax supervision	2	$20,000 (overstated pay)		$20,000	$6,000	Automated Time System, Increased supervisor review	Strong	1	$840	$5,160
Bribery for Maintenance Contracts	Opaque bidding, financial incentives	3	$150,000 (inflated costs)		$150,000	$75,000	Transparent procurement and bidding process, ethics training	Strong	1	$7,500	$67,500

Likelihood:
1: Rare
2: Unlikely
3: Possible
4: Likely
5: Almost Certain

Effectiveness:
Strong: Fully addresses risk
Moderate: Partially addresses
Weak: Minimal Impact

Probability:
1: 10%
2: 30%
3: 50%
4: 70%
5: 90%

EXAMPLE FRAUD RISK PROFILE FOR PROGRAM 1

(2 highest risk fraud schemes)

Potential Fraud Scheme	Falsified Tenant Eligibility	Landlord Overbilling
Description	Tenants or organization staff falsify income, family size, or eligibility data to qualify for vouchers.	Landlords charge organization for higher rents than agreed or for vacant/unoccupied units.
Likelihood	High (Reliance on self-reporting)	Moderate (Weak IC)
Impact	High	Moderate to High
Risk Tolerance	Low	Low to Moderate
Risk Prioritization	1 (Highest) Undermines program mission	2 (High) Critical but secondary
Response Activity	- Implement mandatory Income Verification system checks - Conduct annual recertification audits - Cross check with other federal databases	- Require landlord submission of occupancy logs - Cap payments at FMR levels - Perform random site inspections
Owner	Compliance Officer	Finance Team

Appendix K – Repeat and Expand Fraud Risk Assessments

Step	Action	Procedure	Policy	Customization	Responsibility	Frequency	Outcome
1	Policy Establishment	Define the overarching policy for fraud risk management.	Establish a policy that mandates regular fraud risk assessments, outlines objectives, and sets expectations for risk tolerance.	Tailor policy to reflect the company's culture, industry specifics, and compliance requirements.	Leadership/Senior Management	Upon new policy adoption or significant updates	Comprehensive Fraud Risk Management Policy
2	Risk Identification	Conduct workshops, surveys, or use data analytics to identify potential fraud risks.	Policy requires all departments to actively participate in identifying new or changing fraud risks.	Include unique fraud scenarios pertinent to specific business units, programs, or processes.	Risk Management Team with Departmental Input	Semi-Annually or after significant business changes	Updated list of potential fraud risks
3	Risk Analysis	Analyze each risk for likelihood and impact using established criteria.	Policy mandates using a structured method for risk analysis, possibly including both	Customize the analysis framework to fit organizational data capabilities and risk tolerance.	Finance & Compliance	Annually or as new risks are identified	Detailed risk profile with likelihood and impact assessments

Step	Action	Procedure	Policy	Customization	Responsibility	Frequency	Outcome
			qualitative and quantitative measures.				
4	Risk Scoring	Score risks using a predefined matrix or formula.	Policy dictates how risks are scored, ensuring consistency across assessments.	Adjust scoring parameters to reflect organizational growth, technological changes, or market dynamics.	Risk Management Team	Annually	Scored and prioritized list of fraud risks
5	Risk Prioritization	Prioritize risks based on scores and strategic business impact.	Policy ensures that prioritization aligns with business strategy and resource allocation.	The criteria for prioritization can be tailored to focus on areas like customer trust, regulatory impact, or financial stability.	Leadership	Annually	Actionable priority list for fraud risk management
6	Control Assessment	Evaluate the effectiveness of current controls against identified risks.	Policy requires periodic review of controls to ensure they are up-to-date and effective.	Modify control evaluation to include emerging technologies or new control types (e.g., AI for monitoring).	Internal Audit	Bi-Annually	Report on control effectiveness and gaps

Step	Action	Procedure	Policy	Customization	Responsibility	Frequency	Outcome
7	Mitigation Planning	Develop or revise mitigation strategies for prioritized risks.	Policy enforces that every high or medium risk has a corresponding mitigation plan.	Customize plans to leverage unique organizational strengths or to address specific weaknesses.	Compliance Officer	As per risk prioritization	Detailed and actionable mitigation strategies
8	Implementation & Training	Implement mitigation measures and train staff accordingly.	Policy mandates training on new fraud prevention measures for all relevant employees.	Tailor training toin different roles or departments, possibly including simulation exercises.	HR and Department Heads	After plan development	Enhanced controls and employee awareness
9	Monitoring & Feedback	Set up monitoring systems and gather feedback on control performance.	Policy requires ongoing monitoring with feedback loops to adjust strategies.	Customize KPIs or use department-specific metrics for monitoring.	Risk Management with IT Support	Continuously	Data on control performance and feedback
10	Review & Update	Review the entire fraud risk assessment process.	Policy stipulates a review cycle to ensure the process remains relevant and effective.	Incorporate feedback, industry trends, or regulatory changes into the process update.	Quality Assurance or Risk Management	Annually	Continuous improvement of the fraud risk assessment process

Step	Action	Procedure	Policy	Customization	Responsibility	Frequency	Outcome
11	Reporting	Document and report fraud risk assessment outcomes.	Policy ensures transparency with regular reporting to management and potentially external stakeholders.	Reports can be customized for different audiences, focusing on different aspects of the fraud risk profile.	Compliance or Risk Officer	Annually or upon request	Formal documentation of the fraud risk profile and assessment process

Appendix L – Implement Control Activities

Risk Area	Risk Description	Control Activity	Policies	Procedures	Techniques	Mechanisms	Feedback/Reporting
Procurement	Invoice Fraud - Over-billing or fictitious invoices	Segregation of Duties	Establish a policy where no single individual can authorize, approve, and record transactions.	Require dual signatures for invoice approval. Implement a detailed review process for new vendors. Monthly vendor payment audits.	Use data analytics to identify anomalies in invoice patterns or amounts.	Implement an Enterprise Resource Planning (ERP) system with role-based access controls. Implement automated invoice verification software.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
		Vendor Verification	Policy for mandatory background checks on new vendors.	Regular updates to vendor lists, requiring re-verification every year.	Regular audits of vendor invoices against goods/services received.	Use of a centralized vendor database with verification flags.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
Financial Reporting	Earnings/Income Manipulation - Misstating financial results	Independent Review	Policy mandating external audit by a reputable firm annually.	Internal audit team performs quarterly reviews of financial statements.	Utilization of forensic accounting techniques to detect unusual patterns or adjustments.	Implement automated tools for variance analysis and anomaly detection.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body

Risk Area	Risk Description	Control Activity	Policies	Procedures	Techniques	Mechanisms	Feedback/Reporting
		Whistleblower Program	Establish a policy protecting whistleblowers and encouraging reporting of suspicious activities.	Set up anonymous reporting channels with clear procedures for investigation.	Training on recognizing signs of manipulation for finance staff.	Use of a case management system for tracking whistleblower reports.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
Payroll	Ghost Employees - Payment to non-existent employees	Payroll Reconciliation	Policy requiring reconciliation of payroll with HR records.	Monthly review of payroll against active employment records.	Implement surprise audits or spot checks on payroll.	Use biometric or electronic timekeeping systems to verify employee presence.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
Sales	Revenue Recognition Fraud - Premature or fictitious sales	Credit Checks	Policy for credit checks on new customers before extending credit.	Implement a procedure for periodic review of customer creditworthiness.	Monitor for unusual patterns in customer credit usage.	Employ credit scoring software integrated with sales processes.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
		Data Encryption	Policy to encrypt sensitive data both at rest and in transit.	Regular encryption key management and updates.	Conduct penetration testing to identify vulnerabilities.	Use of encryption software and secure communication protocols.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body

Risk Area	Risk Description	Control Activity	Policies	Procedures	Techniques	Mechanisms	Feedback/Reporting
IT Security	Cyber Fraud - Data breaches leading to fraud	Access Control	Policy defining strict access rights, least privilege principle.	Implement user access reviews semi-annually.	Use of intrusion detection systems to monitor network traffic.	Deploy identity and access management (IAM) solutions.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
		Asset Tracking	Policy for all significant assets to be tagged and tracked.	Regular physical inventories compared against asset registers.	Use RFID or barcode scanning for asset management.	Implement asset management software with real-time tracking capabilities.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
Operations	Asset Misappropriation - Theft or misuse of company assets	Approval for Disposal	Policy requiring multiple approvals for asset disposal.	Log and document all asset disposals with reasons and approvals.	Random checks or audits on asset disposal records.	Use of electronic approval workflows for asset management.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
Grant Program	Fund Monitoring and Approval - Funds allocated for a grant program are used for unauthorized or personal purposes.	Policy requiring strict oversight of grant fund usage, with clear guidelines on allowable expenditures.	Implement a multi-level approval process for grant disbursements and expenditures, including periodic reviews of	Use variance analysis to compare actual expenditures against approved budgets.	Deploy grant management software with real-time tracking and alerts for unusual spending patterns.		OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body

Risk Area	Risk Description	Control Activity	Policies	Procedures	Techniques	Mechanisms	Feedback/Reporting
			fund allocation.				
	Falsified Reporting - Grant recipients submit inaccurate or fabricated reports to misrepresent progress or outcomes.	Reporting Verification	Policy mandating verification of all grant reports against physical or digital evidence of project progress.	Require recipients to submit supporting documentation (e.g., invoices, photos) with reports, followed by random audits.	Apply data analytics to detect inconsistencies or anomalies in reported data.	Use an online reporting portal with built-in validation checks and audit trails.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
	Ineligible Recipients -Grants awarded to individuals or organizations that do not meet eligibility criteria.	Eligibility Screening	Policy for thorough vetting of grant applicants based on specific eligibility criteria.	Conduct background checks, financial reviews, and cross-verification with databases before approving grants.	Employ risk scoring models to evaluate applicant eligibility based on historical data.	Implement a CRM system integrated with public records and databases for automated eligibility checks.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body
	Duplicate Funding - Recipients receive funding for the same project from	Funding Verification	Policy prohibiting duplicate funding without prior	Require applicants to disclose all funding sources and verify this through third-	Use data matching techniques to identify overlapping funding	Use a centralized grant tracking database to monitor and	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body

Risk Area	Risk Description	Control Activity	Policies	Procedures	Techniques	Mechanisms	Feedback/Reporting
	multiple grant sources without disclosure.		approval and full disclosure.	party checks or databases.	requests across programs.	flag duplicate applications.	
	Intentional Non-Compliance with Grant Terms - Recipients intentionally fail to adhere to grant terms, timelines, or reporting requirements.	Compliance Monitoring	Policy requiring ongoing compliance checks throughout the grant period.	Schedule regular compliance reviews and site visits to ensure adherence to grant terms.	Conduct trend analysis on compliance data to identify early warning signs of non-compliance.	Deploy a compliance management system with automated reminders and dashboards for tracking deadlines and requirements.	OIG/ Law Enforcement/ DOJ/ FBI/ External Investigative Body

Appendix M– Acting on Potential Fraud

Step	Action	Description	Responsibility	Timeline Examples	Examples of Possible Outcomes
Fraud Identification and Tracking	Incident Reporting	Document and classify potential fraud incidents reported via whistleblower channels or monitoring.	Compliance Officer	Within 24 hours	Confirmed fraud incidents documented
Investigation	Detailed Investigation	Conduct in-depth analysis to verify fraud, gather evidence, and assess impact.	Internal Audit / IT	5-10 business days	Investigation report with evidence
Process Review	Evaluate Existing Processes	Review processes related to the exploited vulnerability to identify gaps.	Process Owners	15-30 days	Process gaps identified and documented
Control Enhancement	Implement New Controls	Design and deploy enhanced controls to address vulnerabilities and prevent recurrence.	Risk Management / IT	30-60 days	Enhanced controls implemented
Policy Update	Revise Fraud Policies	Update or create policies to reflect lessons learned and prevent similar frauds.	Legal / Compliance Team	30-45 days	Updated fraud policies documented
Procedure Modification	Update Operational Procedures	Modify procedures to incorporate new controls and mitigate risks.	Process Owners	30-60 days	Updated procedures in place

Step	Action	Description	Responsibility	Timeline Examples	Examples of Possible Outcomes
Training & Awareness	Employee Training	Conduct training on new policies, procedures, and fraud prevention techniques.	HR / Training Department	Within 60 days	Improved employee awareness
Monitoring & Testing	Ongoing Monitoring	Continuously monitor and test controls to ensure effectiveness and adapt to new risks.	Risk Management / Audit	Continuously (Quarterly Reviews)	Control effectiveness metrics
Reporting & Feedback	Stakeholder Reporting	Document actions, report to senior management, and establish a feedback loop for improvement.	Chief Risk Officer	Quarterly or as needed	Improved transparency and process refinement

Appendix N – Measuring Effectiveness

Category/Phase	Description	Indicators	Evaluation Process	Evidence of Evaluation	Adjustments/Updates
Fraud Risk Policies	Clear, documented policies outlining fraud prevention and detection objectives and procedures.	- Policy Adoption - Employee Acknowledgement - Frequency of policy updates	- Annual Policy Review - Employee awareness surveys - Compliance audits	- Signed policy acknowledgement forms - Audit reports - Policy revision/update logs	- Update policies based on audit findings - Include new fraud trends identified
Prevention Activities	Proactive measures (e.g., training, segregation of duties) to reduce fraud opportunities.	- Number of trainings held - Number of training attendees/rate - I/C compliance rate	- Training assessments - Internal control testing - Risk assessment frequency	- Training Records - Internal control test results - Risk assessment report/results/scores	- Enhanced opportunities for training. - Adjust controls in accordance with risk evolution
Detection Activities	Reactive measures (e.g., audits, whistleblower hotlines) to identify fraud incidents.	- Number and scope of audits conducted. - Hotline reports received - Lag time (occurrence to detection)	- Analysis of audit findings - Identified trends in hotline reports - Incident response time	- Audit summary/response - Hotline call logs - Incident response documentation	- Increased audits/frequency - Improve hotline visibility if underutilized

Category/Phase	Description	Indicators	Evaluation Process	Evidence of Evaluation	Adjustments/Updates
Monitoring Process	Ongoing oversight to ensure prevention/detection activities remain effective.	- Frequency of monitoring reviews - Number of issues identified - Resolution rate	- Regular management reviews - KPI tracking - Comparisons to industry standards	- Monitoring reports -Key Performance Indicator (KPI) results analysis - Comparison analysis	- Adjust monitoring frequency - Address unresolved issues
Overall Effectiveness Evaluation	Assessing how well activities mitigate fraud risks based on outcomes and feedback.	- Fraud incidents detected - Loss amount prevented	- Post incident reviews/lessons learned - Cost/benefit analysis	- Post incident reports - Financial impact analysis/reports	- Fine tune prevention processes - Adjust for negative impacts

Appendix O – Sources

1. GAO A framework for Managing Fraud Risks in Federal Programs, July 2015 GAO-15-593SP, A Framework for Managing Fraud Risks in Federal Programs
2. CFO Antifraud Playbook Interactive-Treasury-Playbook.pdf
3. New Zealand Serious Fraud Office Fraud Risk Assessment: Good Practice Guide, October 2024 Fraud Risk Assessment Good Practice Guide
4. Chartered Institute of Management Accountants Fraud Risk Management; A Guide to Good Practice, January 2009 Fraud risk management: a guide to good practice
5. Information Systems Audit and Control Association Risk Assessment and Analysis Methods: Qualitative and Quantitative, April 2021 2021 Volume 2 Risk Assessment and Analysis Methods
6. The Institute of Internal Auditors, The American Institute of Certified Public Accountants, Association of Certified Fraud Examiners Managing the Business Risk of Fraud: A Practical Guide managing the business risk of fraud a practical guide.pdf
7. Audit Board, What Is a Fraud Risk Assessment? And Why Do I Need One?, July 2024 What Is a Fraud Risk Assessment? And Why Do I Need One?
8. Audit Board, Risk Assessment Matrix: Overview and Guide, February 2024 Risk Assessment Matrix: Overview and Guide
9. Fraud.com What is Risk Management and its role in combatting Fraud What is risk management and its role in combatting fraud | Fraud.com
10. KPMG Fraud Risk Management: Developing a Strategy for Prevention, Detection and Response, May 2014 Fraud risk management Developing a strategy for prevention, detection and response
11. Linford & Co, LLP Considerations for Fraud Risk Assessment: COSO Principle 8 Understanding Fraud Risk Assessment: COSO Principle 8
12. Research Project for Emerging Issues/Advanced Topics Course Master of Forensic Accounting Program University of Toronto: Fraud Risk Management: Discussion on an Effective Fraud Risk Management Framework, Challenges and Trends, June 2022 download
13. Office of the Auditor General of Canada: Guide on Managing Fraud Risks at the Office of the Auditor General of Canada Guide on Managing Fraud Risks at the Office of the Auditor General of Canada
14. GOV.UK Public Sector Fraud Authority, Professional Standards and Guidance for Fraud Risk Assessment in Government Professional standards and guidance for fraud risk assessment in government (HTML) - GOV.UK
15. Deloitte and Touche COSO Risk Assessment in Practice, October 2012 Riskassessmentinpractice.pdf

16. GRF CPAs & Advisors Creating an Effective Mission Statement, November 2017 Creating an Effective Mission Statement - GRF CPAs & Advisors
17. Aevitium.com How to Develop a Strategic Risk Vision Statement for Your Organization, December 2023 How to Develop a Strategic Risk Vision | Step-by-Step Guide for CROs
18. Institute of Directors Code of Conduct, December 2024 Code of Conduct | Factsheets | IoD
19. GAO Standards for Internal Control in the Federal Government, September 2014 GAO-14-704G, STANDARDS FOR INTERNAL CONTROL IN THE FEDERAL GOVERNMENT
20. GAO Antifraud Resource (https://antifraud.gaoinnovations.gov/resources)