BRIDGING THE GAP FROM ENTERPRISE RISK MANAGEMENT TO ACHIEVING MISSION OBJECTIVES: FRAUD RISK MANAGEMENT

Council of the Inspectors General on Integrity and Efficiency (CIGIE) 2019 Federal Audit Executive Council (FAEC) Annual Conference

September 6, 2019

Dan Kaneshiro
Senior Policy Analyst
OFFICE OF MANAGEMENT AND BUDGET
One of the value propositions of Enterprise Risk Management (ERM) is even in early stages of maturity, it can drive the following two things:

1) Risk-Informed Discussions
2) Risk-Informed Decisions
Overview:

- **7 Cyclical Components**
  - Establish the Context
  - Identify Risks
  - Analyze and Evaluate
  - Develop Alternatives
  - Respond to Risks
  - Monitor and Review
  - Continuous Risk Identification and Awareness

- **3 Enterprise Components**
  - Communicate and Learn
  - Extended Enterprise
  - Risk Environment/Context
III. Establishing and Operating An Effective System of Internal Control.
   • Establishing Entity Level Control.
     • Managing Fraud Risk in Federal Programs.

• **Risk Profiles** – Agencies must include an evaluation of fraud risks including:
  • Fraud as defined by the GAO Green Book.
  • A risk-based approach to design and implement financial and administrative control activities to mitigate identified material fraud risks.
  • Fraud risk may be organized under the operational objectives of the risk profile.
  • Agencies may determine that they have low likelihood or impact of fraud.
• **GAO Fraud Risk Framework** – Agencies should adhere to leading practices when:
  • Establishing entity level controls.
  • Establishing risk tolerances in disaster situations.

VII. Other Considerations.

• Agencies must consider fraud risk in strategic plans and ensure appropriate officials receive training on fraud indicators and risks related to:
  • Conducting Acquisition Assessments.
  • Managing Grant Risks in Federal Programs.
Join the FRDAA-WG TODAY

I WANT YOU TO KICK FRAUD
Risk Appetite

- The broad-based amount of risk an organization is willing to accept in pursuit of its mission/vision.
- Established by the organization’s most senior level leadership.
- Serves as the guidepost to set strategy and select objectives.

Risk Tolerance

- Acceptable level of variance in performance relative to the achievement of objectives.
- Established at the program, objective or component level.
- Management considers the relative importance of the related objectives and aligns risk tolerance with risk appetite.
The **GAO Fraud Risk Management Framework** includes an example of Risk Tolerance and Risk Matrices in the Context of Natural Disaster Assistance which both aligns and complements current guidance in **A-123** and **M-18-14**.

- **A-123 and M-18-14**: “Risk tolerance reflects a Federal manager's willingness to accept a higher level of fraud risks and may vary depending on the circumstances of the program.”

- **A-123 and M-18-14**: “When determining risk tolerances in disaster situations, managers must weigh the program's operational objectives against the objective of lowering the likelihood of fraud.”
Innovation

Efficiency

Compliance

Non-Compliance

The House With a Basement and an Attic
Questions

Dan Kaneshiro DKaneshiro@omb.eop.gov
Together We Can Be More Effective In Addressing Improper Payments including Fraud

September 6, 2019
Program Integrity

Program Integrity

Focus of the Antifraud Playbook

Internal Controls

Payment Integrity

Improper Payments Prevention

Enterprise Risk Management (ERM)
The Antifraud Playbook Contents

16 Antifraud Plays Organized into Four Phases

https://cfo.gov/fraudprevention
Play 5 Think Like a Fraudster

Fraud Risk Map Example
Fraud creates “leaks” of funding, reducing available funds for legitimate activities

SCHEME
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.

ACTORS

The Nonfinancial Impact of Fraud
Fraud encompasses the loss of anything of value, even non-financial value - such as PHI - which can create other risks, such as reputational, compliance, or operational failures and challenges.

SCHEME
Employees pad time sheets, usually in small enough increments to escape the notice of supervisors.

ACTORS

SCHEME
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.

ACTORS

Payroll Staff
Employee
Play 6 – Discover What You Don't Know

GAO Guidance

1. Identify inherent fraud risks

2. Assess likelihood and impact of inherent risks

3. Determine fraud risk tolerance

4. Determine and prioritize residual fraud risks

5. Document program's fraud risk profile

Playbook Checklist

- Leverage your Fraud Risk Map (See Play 6) to understand the potential entry points for fraud.
- Identify your preferred risk assessment technique (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
  - Determine the likelihood and impact of given schemes being successful

For example, you could conduct focus groups with stakeholders that know the controls and processes related to the fraud schemes you plan to assess, and discuss the controls and processes in place related to the fraud schemes identified, the strengths of those controls, and the potential likelihood and impact of the schemes.

- Document the results of your risk assessment. For example, you can document high likelihood and impact scores for given fraud schemes in addition to any identified controls gaps in your Fraud Risk Map (See Illustration).

- 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 might identify include:
  - Contracts bill for goods or services that were not provided, which results in financial loss to the agency
  - Contracts 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 still pull the specific risk associated with the scheme. In the examples above, the risks identified was financial loss, but it can be anything you may discuss or identify in your assessment as a potential risk of the particular fraud scheme.

- Prioritize risks based on the results of the assessment. For example, you can prioritize risks based on likelihood and impact scores or strategic priorities.

Note: We recommend focusing on residual risks at this stage because these are the risks you will be focused on mitigating, see Key Points.

- Establish thresholds above which the component (See Play 8) you are assessing feels it is necessary, from a cost or reputation standpoint, to avoid and what you are willing to accept or share in terms of fraud risk.

Note: You will never get to “zero” fraud, so you may decide not to dedicate resources to risks that are deemed unlikely or low impact.

- Document prioritized risks including key pieces of information such as the likelihood and impact score, the existing controls, any identified gaps, and responses to mitigation activities - you will put in place to address the risks.

- Document your fraud risk profile based on your risk tolerance, prioritized risks and overall results of the assessment process.
Payment Integrity Center of Excellence

VISION

to be a trusted Governmentwide partner to provide actionable business insights and solutions that transform how Government agencies approach identification, prevention, stopping, and recovery of improper payments and related fraudulent activity.

MISSION

to provide Governmentwide partnership, guidance, and solutions that aid in the prevention of improper payments and fraud, waste and abuse.

GOALS

Improve the integrity of Government-wide financial transactions by providing business insight and solutions that assist Government agencies in identifying, preventing, and recovering improper payments.
Payment Integrity Throughout the Payment Lifecycle

1. **Identify Improper Payments**
   - Identify the payment or payee that should not be paid

2. **Prevent (Pre-Award, Pre-Payment)**
   - Prevent the award or payment before sending to Treasury

3. **Recall (At time of Payment)**
   - Hold for further analysis or cancel payment before disbursement

4. **Recover (Post-Payment)**
   - Request recovery of funds from the Financial Institution

5. **Investigate**
   - Refer for investigation if criminal activity is determined

6. **Share**
   - Share outcomes and discoveries with stakeholder community

**Identify people who shouldn’t be paid & payments that should not have been made**
Payment Integrity Solution Lifecycle

**1. UNDERSTAND BUSINESS PROBLEM**
Collaborate with customers, understand business needs

**2. DEVELOP CUSTOMER-CENTRIC SOLUTION**
Develop innovative analytical solutions with business insights

**3. IMPLEMENT SOLUTION**
Provide actionable and tangible outcomes that solve operational business problems.

**4. MEASURE VALUE**
Evaluate results and effectiveness of process improvements

**5. IMPROVE**
Share best practices with stakeholders through training and outreach

---

**Repeatable process for development of Payment Integrity Solutions**

---

**PAYMENT INTEGRITY CENTER**

---

**LEAD • TRANSFORM • DELIVER**
Payment Integrity Info-Apps In Action

Agencies and IGs have Payment Integrity Questions…

Problem: Zip Codes identified as “at risk” for theft
Solution: Zip Code / Check Number View

Problem: Apartment building identified as “suspect”
Solution: Address View

Problem: SSN identified as victim of identity theft
Solution: Payee View

Problem: Increased fraud suspected on a given RTN
Solution: Bank View

Problem: Hurricane requiring monitoring of a geographic region
Solution: Agency Geographic View

Info-Apps have answers!
Payment Integrity Info-Apps in Action

Users supply parameters such as date range, agency, and event to monitor.

Info-App provides post payment monitoring and alerts for disaster event.

Alerts identify payment integrity risks (e.g. Many payees at one address, possible forgeries).

User can drill down for a list of payees with uncashed or returned checks.

Monitor Payees Impacted by Natural Disasters

Begin Date: 09/01/2017
End Date: 09/16/2018
Agency: ALL

Event:
- FLORIDA
- Harvey Hurricane
- Irma Disaster
- Maria Hurricane
- mudslides

Alerts:
- Many payees at one address, possible forgeries

User interface with data tables and summaries.
# High Dollar Payments to High Fraud Risk Financial Institutions

| Problem | Agency discovered fraudulent large dollar payments disbursed to pre-paid debit cards:  
|• Payees may be unaware of identity theft and payments made on their behalf 
|• Payments may be misdirected or unauthorized / non-entitled 
|• Agencies may be unaware of high-risk RTN with high percentage of fraud |

| Solution | Info-App monitors high dollar payments to Financial Institutions with high risk of fraud:  
|• List of FIs maintained through network of agencies and law enforcement 
|• Identified payments over $5K to high-risk FIs 
|• Identified fraud indicators (return reasons, non-receipts claims, fraudulent enrollments) 
|• Conducted payee profile analysis (Have other agencies paid this person to the same FI?) |

| Results | Provided cross governmental payee profile risk analysis:  
|• Conducted pilot with several agencies to test cross-government data sharing 
|• Analyzed fraud trends (RTN, geographic area, payment types) 
|• Worked with agency stakeholders and IGs to identify, recover, and investigate |
Common Challenges

How can we partner to solve Payment Integrity issues?

Seven Topics of Common Interest

- Payments to the Deceased
- Inter-Agency Benefit Eligibility
- Payee Validation (Banking Info, Address)
- High Risk Financial Institutions
- Compromised Payees and Accounts
- Payee Characteristics (DOB, DOD, Incarcerated, etc.)
- Updates to 31 CFR Part 210
Deceased Payee Analysis

Step 1 – Understand the Business Problem

How can we prevent Payments to the Deceased?

How big is the problem?
Identify payments made after date of death

Compile data sources
Utilize multiple sources of deceased payee data

Who is paying them?
Identify agencies and payment types

Data Quality Analysis
Evaluate payees and dates of death to ensure consistent info

Evaluate eligibility rules
Determine if payments to deceased individuals were appropriate

Recovery Efforts
Determine if funds were recovered from post payment events
What’s Next?

Agency Partnership Engagement
- Quarterly Meetings
- Review cross government initiatives
- Solicit agency requirements
- Share best practices

OMB Workgroups
- Participate in CAP Goal 9 Workgroups
  - Strategic Data Use
  - Monetary Loss – Root Causes
- Provide subject matter expertise

Implement Customer Solutions
- Initiate Customer Driven Projects
- Apply repeatable Payment Integrity Solution Lifecycle
- Utilize core competencies to execute solutions
- Demonstrate tangible value through prevention and recovery
Established a DHS OIG Anti-Fraud Plan

Launch of Specialized Units

Strategic Efforts:

• *Create a Culture of Anti-Fraud Measures*

• *Work with DHS to Identify and Assess fraud risks*

• *Implement internal and external mechanisms for Preventing and Detecting fraud*

• *Insight into Actions: indictments, convictions, recoveries and future prevention*

Questions
Anti-Fraud Plan

Mission:

- Proactively identify, investigate and prosecute fraud schemes and corrupt activities that pose significant risk and major financial impact to DHS;

- Develop expertise in every field office and provide highly specialized tools and other support to the field, enabling INV to conduct high impact fraud and corruption cases around the country.
Establish and maintain a multi-disciplinary team of fraud experts:

- Special Agents well-versed in conducting complex fraud investigations
- Forensic Auditors/Forensic Accountants
- Intel Analysts
- Data Scientists
- Digital Forensic Analysts
- Program Analysts
- Admin Support Staff
Collaborate with OIG Audits to help identify high-impact fraud and contract corruption (sensitizes OA to fraud schemes)

Collaborate with OIG & law enforcement community to identify latest schemes

Review DHS OIG Hotline with “Big Fraud Perspective”

Attend fraud conference/forums to identify latest schemes

Meet with DHS stakeholders to identify vulnerabilities

Identify data sources that can be mined
Implement a strong fraud awareness effort throughout DHS

Partner with DHS Office of Chief Procurement Officer and Heads of Contracting Activities

Establish a close partnership with DHS Suspension and Debarment Officials

Develop Fraud Working Groups within DHS

Use analytics to proactively detect significant frauds and corruption
Strategically target, build and conduct major fraud and corruption investigations

- Work with law enforcement counterparts and DoJ to facilitate investigations and prosecutions
- Use specialized fraud expertise to enable DHS OIG field offices throughout the U.S.
- Utilize DHS Component investigative organizations to support fraud investigations
Case Study

Fusion Team Makeup – $100M benefits fraud

- Senior Special Agent
  - Data Scientist (1)
  - Digital Forensics Analyst (1)
  - Intelligence Analyst (2)
  - Forensic Accountant (2)
  - Field Agents (multiple)
Case Study

Contractor Impersonation

- Fraudsters obtain legitimate solicitations
- Fax/Phone/Email and delivery address are replaced
- Sent to contractors
- Fraudsters “accept” and take delivery of products
“There is no kind of dishonesty into which otherwise good people more easily fall than that of defrauding the government.”

- Benjamin Franklin
Contact Information

Office of Management And Budget
Dan Kaneshiro

Bureau of the Fiscal Service
Tammie Johnson
Management and Program Analyst
tammie.johnson@fiscal.treasury.gov
paymentintegrity@fiscal.treasury.gov
304-480-7139

James Long