Now, Next, Beyond – Fighting Fraud in Government Programs

1:05 to 2:45pm ET

24 May 2023

EY
Building a better working world

Agenda

1.	Current Environment	25 mins
2.	Assess Fraud Risks	35 mins
3.	Respond to Fraud Risks	
3.1	Data Analytics for Fraud Prevention and Detection	20 mins
3.2	Approaches & Resources	5 mins
4.	Evaluate & Adapt	5 mins
5.	Questions & Wrap up	10 mins

Key takeaways

- Understand the current fraud trends and challenges associated with fraud prevention and detection.
- Describe leading practices, tools, and techniques for fraud prevention in government programs.

Scott Nemeroff
Executive Director
EY Forensic & Integrity Services

Taylor Larimore
Senior Manager
EY Forensic & Integrity Services

Now, Next, Beyond

Compliance Driven

Value Driven

Now

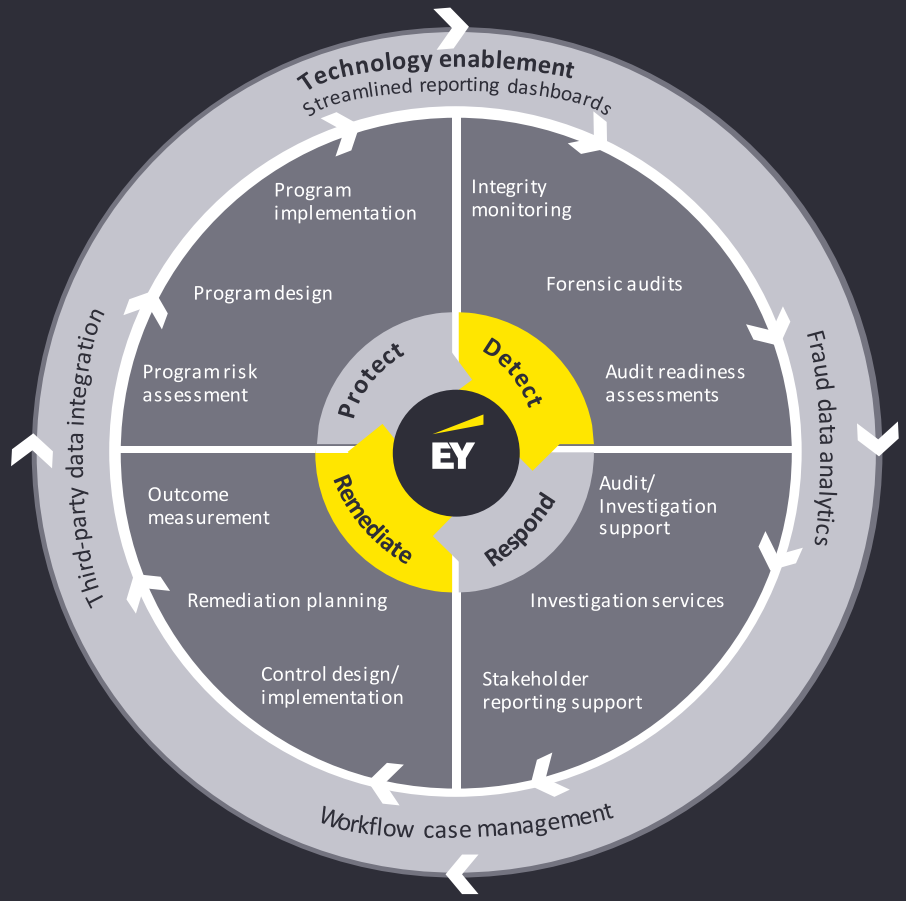
- Identify key risk areas and eligibility requirements
- Data exploration and collection
- Develop analytics to identify fraud risks
- Design and implement policies and procedures
- Capacity assessment
- Add scalable/temporary resources

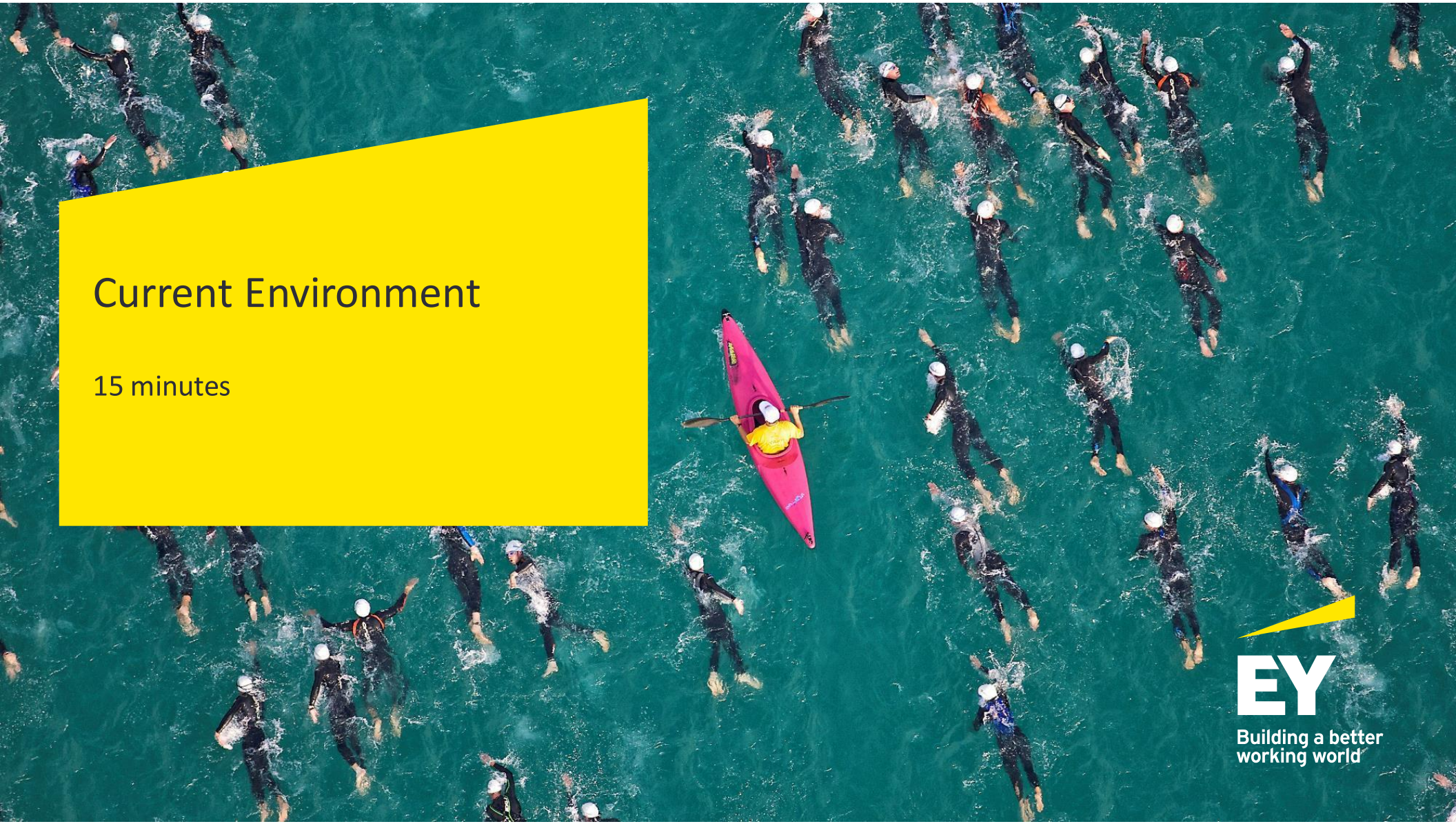
Next

- Enhance fraud analytics solution through automation and advanced analytics
- Deploy case management and workflow solution
- Develop reporting on eligibility and fraud for regulators and executives
- Identify potential third-party data sets of interest
- Monitor planning/implementation

Beyond

- Risk-based prioritization of fraud investigations and assessments
- Machine learning to train analytics based on confirmed eligibility or fraud cases
- Integrate with third-party data
- Streamline reporting, investigations and reviews
- React to audit findings
- Investigate potential fraud, waste and abuse





Current Environment

15 minutes

Building a better working world

Current Environment
Challenges for Government Programs

Common operational challenges facing governments:

- There is a lack of capacity and resources to support a temporary program surge.
- Complexity of subrecipient and third-party relationships require enhanced scrutiny.
- Siloed environment and regulatory hurdles limit collaboration, data sharing, and effective oversight.
- Minimal documentation to support compliance, controls and decisions leads to audit challenges.
- Size and scale of programs was much larger in scale then previous or active programs.
- Aid was distributed though new funding mechanisms for which some agencies (fed and state) had little experience.
- There is a lack of infrastructure and experience responding to inquiries from state and federal oversight bodies.
- FRM procedures are viewed as a check-the-box compliance effort rather than an opportunity to drive value and mission success.

Current Environment

Whitehouse Anti-fraud Proposal – Background

- Past underinvestment in basic government technology and the rush of demand for pandemic combined with decision to remove basic anti-fraud controls led to historic fraud and identify theft of emergency benefit funds
- March 2023, President Biden announced a three-part $1.8B proposal that will impact Federal, State and local governments;
  1. $600M to ensure resources and time for investigations and prosecutions of major and systemic pandemic fraud
  2. $600M to invest in preventative measures to mitigate fraud and identify theft
  3. $400M to assist victims of identity theft
- The proposal outlines the use of future legislation and executive orders to provide funding and actions for both Federal and State/Local governments to investigate and prosecute fraud and invest in methods and technology to better mitigate the risk of fraud and identify theft in the future. Primarily the proposals anticipates:
  - Increase funding to certain federal inspector generals, prosecutors, forfeiture and pandemic task forces/watch dogs to investigate, prosecute and recover funds
  - Increase statute of limitations on certain pandemic programs to 10 years to align with other pandemic programs
  - Establish tools, incentives and methodologies of data sharing across federal and state governments to enhance the ability to identify multi-program and multi-fraud and identity theft

Current Environment
Whitehouse Anti-fraud Proposal – Key Takeaways

Increased resources for investigations

- Continued focus by the Biden administration to prioritize the fight against fraud, waste and abuse dating back to TARP
- Recognition of under funded investigators, prosecutors and watchdogs
- More investigations will be coming
- Setting precedent that investigations and prosecutions will be on going for at least another 10 years
- The ROI of the investment into investigations is expected to be 10:1

Prioritization of prevention of fraud and identify theft

- The "Pay and Chase Model" is more costly to the taxpayer than investing in proactive measures
- Identity theft is a significant issue that is impacting the country especially in individual assistance programs
- Recognition of the limitations on governments to be proactive without more effective tools that share data across the government landscape specifically with identify theft
- Now is the time to invest in technologies to prevent and detect fraud proactively
- The government is incentivizing states to enhance the methods and tools by allowing states to keep recovered funds to invest in their anti-fraud controls

Current Environment

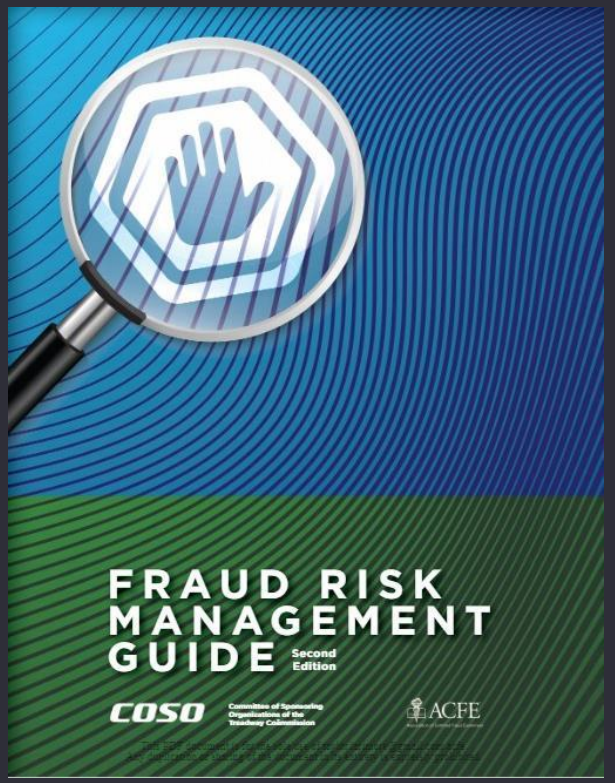
Pandemic Response Accountability Committee Lessons Learned

Lesson 1	Self-certified information needs to be validated before payments are sent
Lesson 2	Prioritize funding for underserved communities
Lesson 3	Use existing federal data sources to determine benefits eligibility
Lesson 4	Recipients and administrators need timely and clear guidance to get benefits out efficiently and accurately
Lesson 5	Recipients of relief funds should be fully disclosed to the public
Lesson 6	Allocate funding based on need
Lesson 7	New programs need more outreach to increase public awareness and participation
Lesson 8	Watchdogs need access to data to find fraud
Lesson 9	Collaboration is critical to oversee pandemic relief programs
Lesson 10	Better reporting is needed to track pandemic relief spending

Source: Lessons Learned (pandemicoversight.gov)

Current Environment
2023 COSO and ACFE Fraud Risk Management Guide Update

- Second Edition was released on May 2, 2023
  - Five Principles for Fraud Risk Management
    - Fraud Risk Governance
    - Fraud Risk Assessment
    - Fraud Control Activities
    - Fraud Investigation and Corrective Action
    - Fraud Risk Management Monitoring Activity
  - What's New?
    - Emphasis on fraud deterrence
      - Expanded fraud risk assessment
      - Enhanced reporting systems
    - Expanded data analytics focus
    - New fraud risks



Source: Product Detail Page (acfe.com)

Current Environment
Recent Fraud Risk Trends

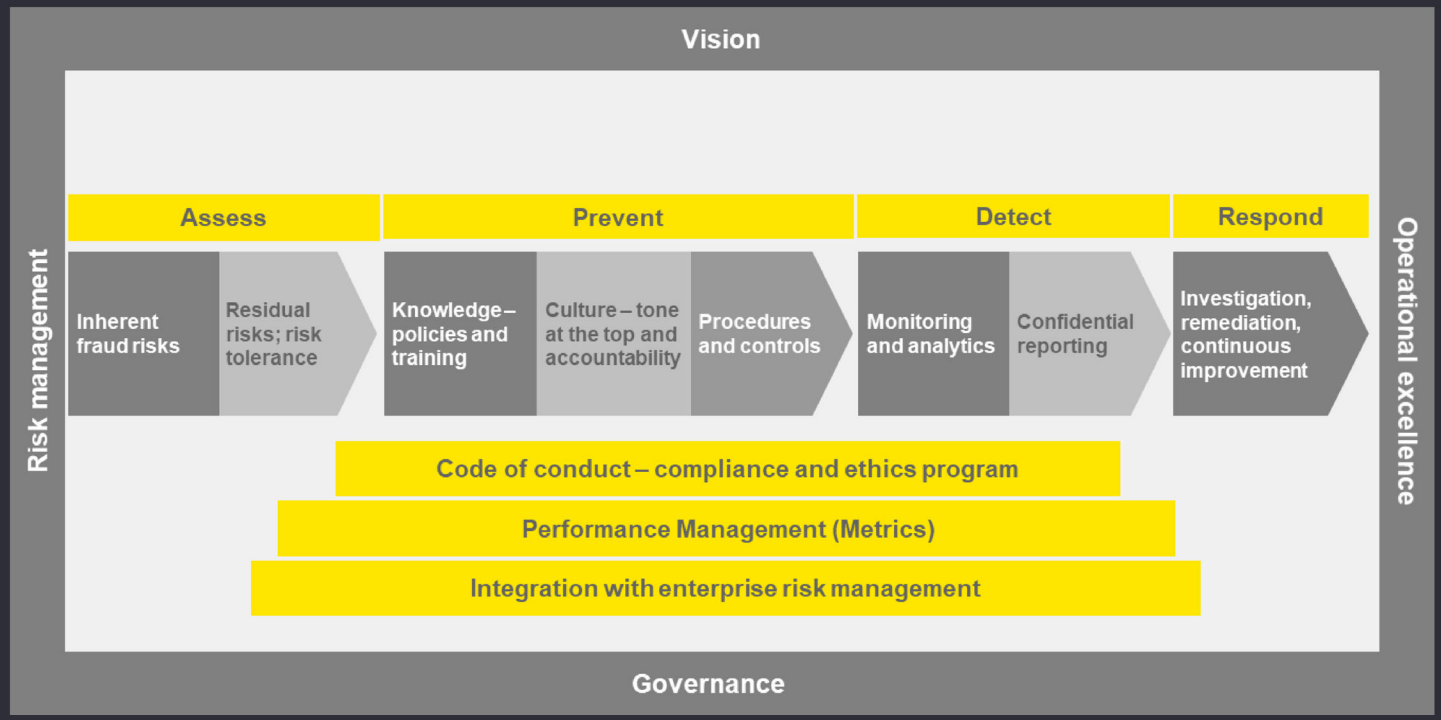
- Identity theft
- Environmental, Social, and Governance (ESG) initiatives and reporting
- Fraud in the cyber channel
- Remote working and hybrid work environments
- Managing fraud risk as a value driver

Assess Fraud Risks

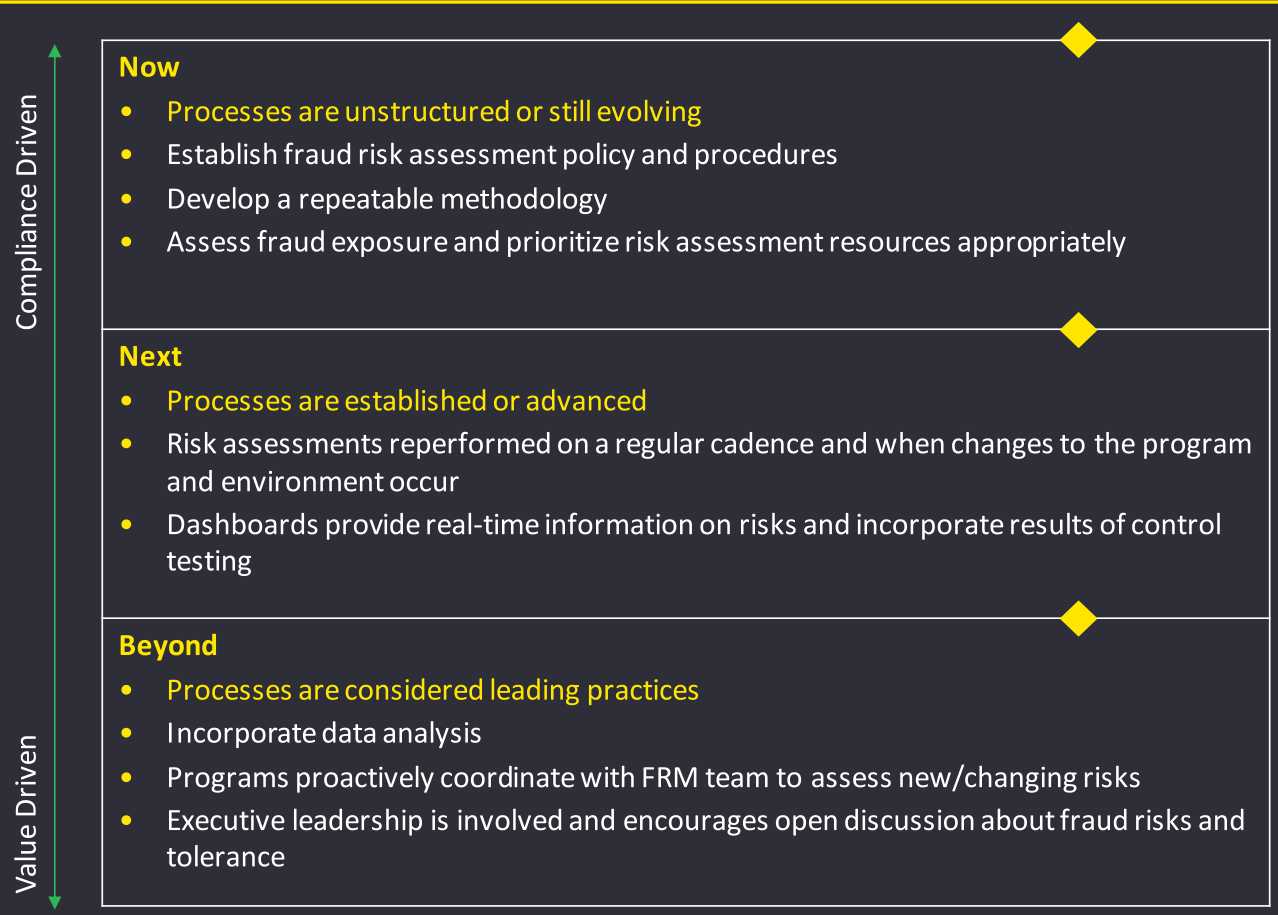
30 minutes

EY
Building a better working world

Examine your current anti-fraud program



Assess Fraud Risks



Fraud Risk Assessment

Challenges and opportunities for anti-fraud leaders

New Challenges

- Defining the impact of fraud "to the achievement of objectives"
- Aligning fraud risk assessment with enterprise risk assessment
- Assessing and managing fraud risks that do not meet the COSO standard of potential impact

New Opportunities

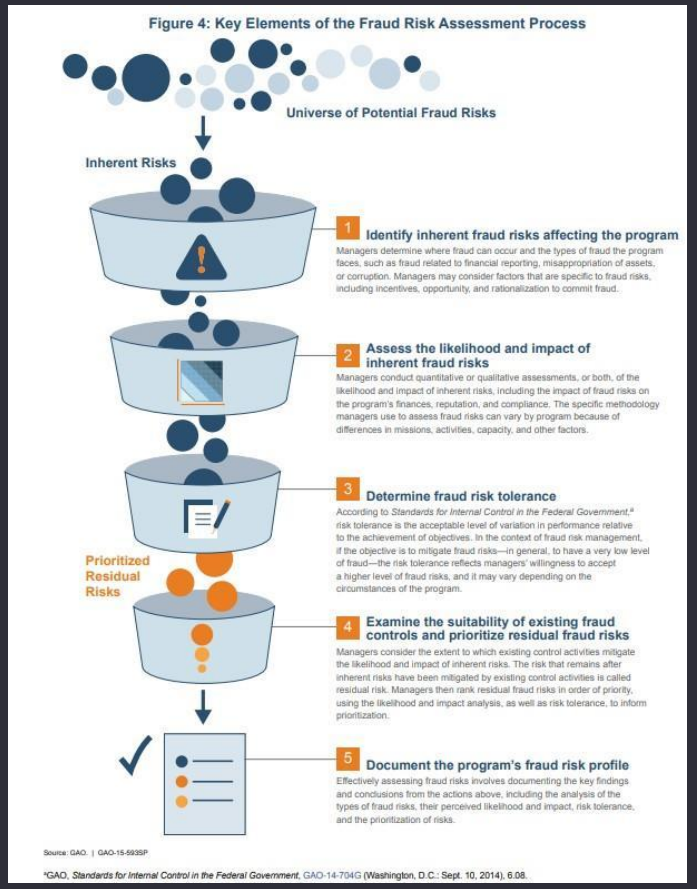
- Re-thinking the agency's most significant vulnerabilities
- Engaging senior management on the topic of fraud and trends
- Rigorous risk-based approach to resource allocation; review of control effectiveness

Solutions

- Methodical approach to identify fraud risks in each program or business process
- Facilitated by rich examples of fraud schemes, red flags and controls
- Risk-based approach to prioritize anti-fraud activities
- Monitoring
  - Emerging risks
  - Controls effectiveness
  - Trends analysis, advanced analytics

Fraud Risk Assessment
Guidance & Best Practices

- Government Accountability Office
  - Green Book
  - Framework for Managing Fraud Risks in Federal Programs
  - Antifraud Resource
- Playbooks & Toolkits
  - ACFE Anti-fraud Playbook
  - ACFE Resources (fraud prevention check-up, fraud risk tools, etc.)
  - Treasury and Chief Financial Officer Council's Program Integrity: The Antifraud Playbook
  - AGA Fraud Prevention Toolkit
- COSO
  - Fraud Risk Management Guide



Fraud Risk Assessment
Fraud vs. Fraud Risk

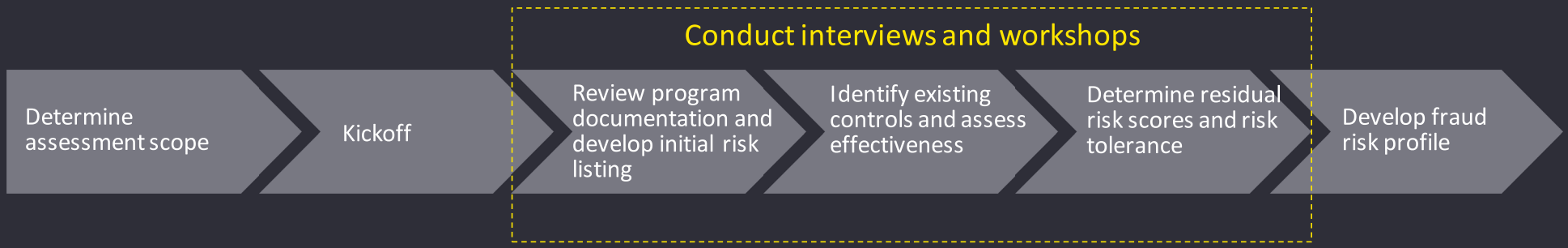
Fraud

Obtaining something of value through willful misrepresentation. Fraud must be determined through the judicial or other adjudicative system.

Fraud Risk

Risk of unexpected financial, material, or reputational loss as the result of fraudulent action of persons internal or external to the organization. When fraud risks can be identified and mitigated, fraud may be less likely to occur.

Fraud Risk Assessment
Approach



Fraud Risk Assessment

Step 1: Determine assessment scope

Consider your fraud exposure	• Look for previous OIG, GAO, audit reports, and instances of known fraud • Program size, complexity, and history • Consult CFO, CRO
Internal vs external fraud	• Consider both external and internal fraud threats
Consider organizational structure	• Assess business cycles or departments/programs
Review applicable guidance and regulations	• GAO Green Book • GAO Fraud Risk Framework • COSO Fraud Risk Management Guide • ACFE Anti-fraud Playbook • Treasury Anti-fraud Playbook

Fraud Risk Assessment
Step 2: Kickoff

Identify key stakeholders	• Include both leadership and staff from business functional areas and programs that will be involved in the risk assessment • Consider whether you need to meet with leadership for buy-in to the process before holding a broader kickoff meeting
Establish clear expectations for roles and responsibilities, level of involvement, and next steps	• Develop a participant guide as a key resource for those with a role in the risk assessment process
Discuss timeline and next steps	• Consider "blackout" periods that align to busy cycles for process owners (e.g., month-end close, payroll processing, asset inventory)

Fraud Risk Assessment

Step 3: Review Program Documentation and Develop Initial Risk Listing

Consider both internal and external fraud threats	• Don't assume that everybody in your organization is honest and following the rules
Start with audit and oversight reports, known fraud cases	• Previously identified fraud and fraud risks will jump start the brainstorming process
Consider fraud entry points and actors	• The controls and responses to fraud risks may vary based on the entry points and actors involved, so it's helpful to think about them separately
Leverage tools and resources	• ACFE, AGA, COSO, GAO have valuable tools, templates, and resources that can improve the assessment
Consider non-financial fraud	• Fraud risks can create risks with a non-financial impact (e.g., health and safety, national security)
Think Like a Fraudster!	• Brainstorm with teams that understand the processes and controls to identify creative fraud schemes that have been previously unidentified

Fraud Risk Assessment
GAO Antifraud Resource

- Benefits of GAO Antifraud Resource:
  - Conceptual fraud model provides a standardized terminology and approach for categorizing and assessing fraud schemes
    - E.g., scheme participants, fraud activity, mechanism, and impact are all defined consistently
  - Provides a rich database of 450+ fraud schemes searchable by:
    - Program area (e.g., transportation, healthcare)
    - Group served or overseen (e.g., contractors, beneficiaries, public utilities, patients)
    - Program service types (e.g., disaster assistance, direct payments, grants)
    - Revenue collected (less common)
    - Agency
    - Fraud type (e.g., beneficiary fraud, procurement fraud, grant fraud)

Antifraud Resource (gaoinnovations.gov)

Fraud Risk Assessment

Step 4: Identify existing Controls and Assess Effectiveness

Collaborate with internal audit to collect control information	• Consider results of test of design and effectiveness testing
Conduct interviews and workshops	• Use interviews and workshops to validate controls and determine effectiveness • Identify control gaps to be addressed
Leverage tools and resources	• ACFE provides lists of anti-fraud controls for core business functions

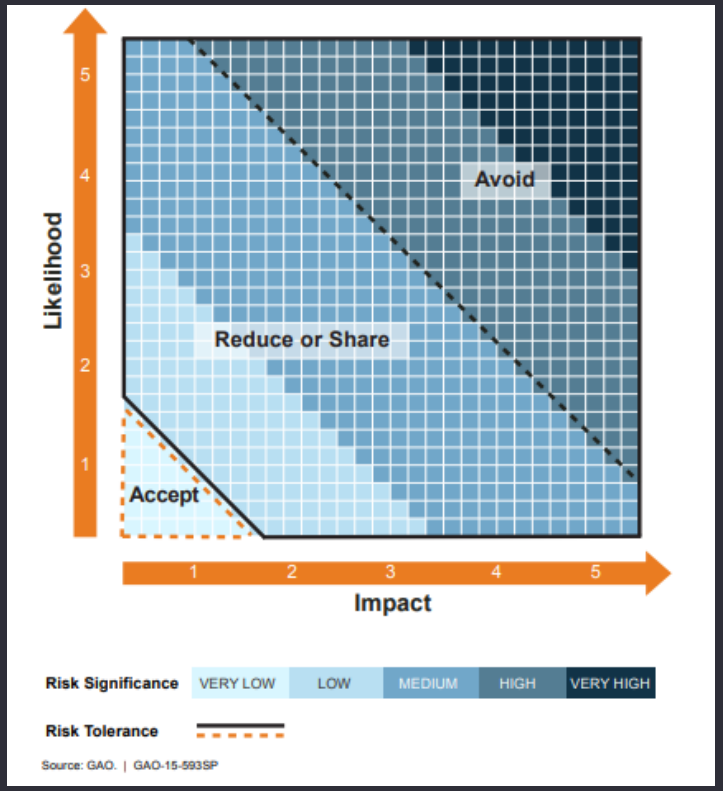
Fraud Risk Assessment

Step 5: Determine Residual Risk Scores and Risk Tolerance

Residual risk: the risk that remains after inherent risks have been mitigated by existing control activities

The responses to fraud risks may include actions to accept, reduce, share, or avoid the risk

The risk of fraud will only be zero if the program doesn't exist – tolerances need to be realistic



Fraud Risk Assessment

Step 6: Document the program's fraud risk profile

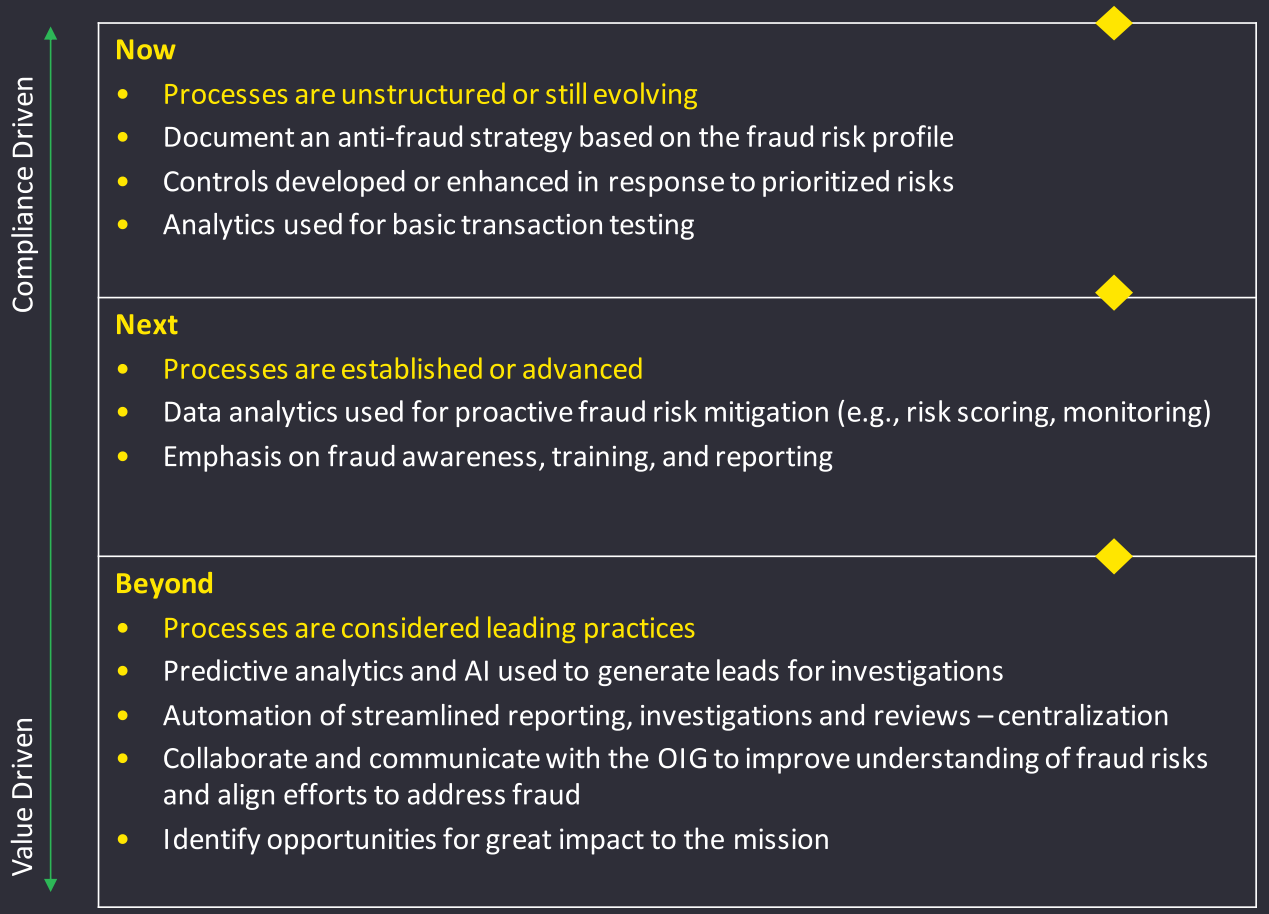
- The fraud risk profile documents the key findings and conclusions from the risk assessment, including the following:
  - Categories of fraud – refer to ACFE Fraud Tree or GAO Antifraud Resource for common terminology
  - Analysis of the types of internal and external fraud risks,
  - Likelihood and impact risk scores,
  - Managers' risk tolerance, and
  - Prioritization of risks.

Respond to Fraud Risks

20 minutes

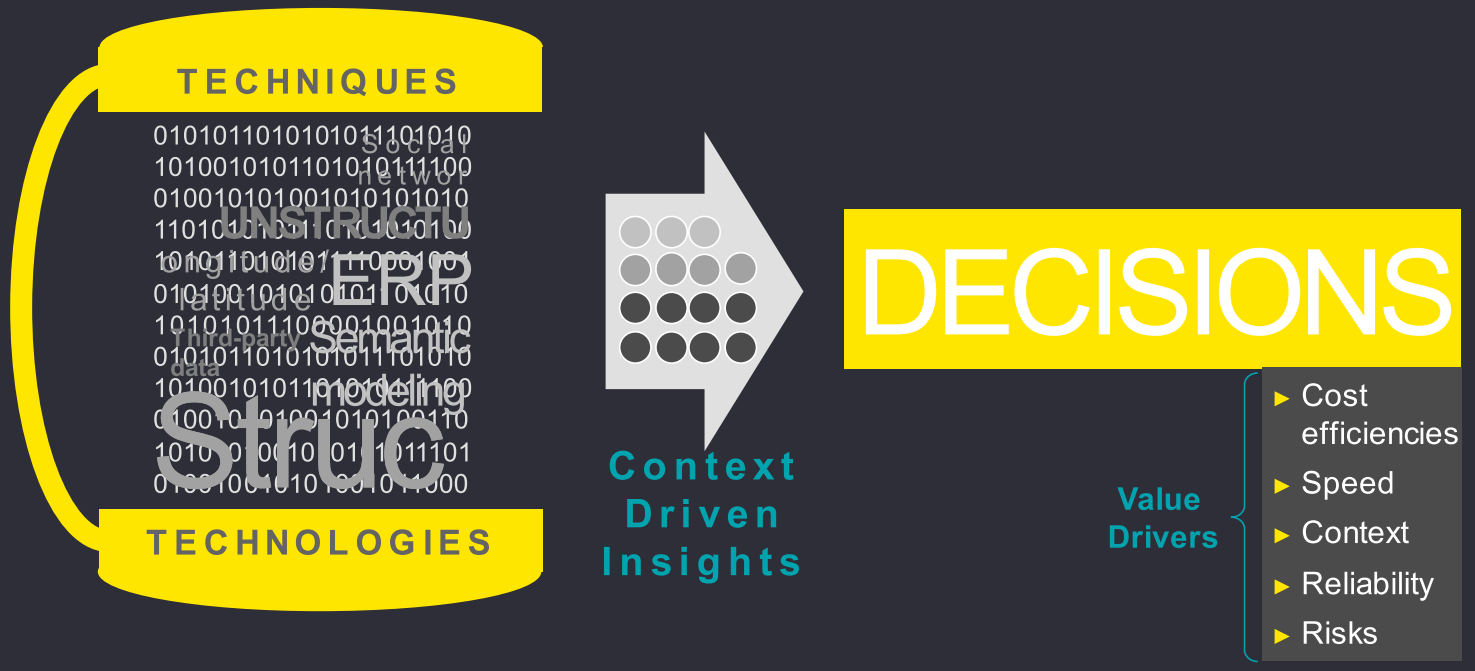
EY
Building a better working world

Respond to Fraud Risks

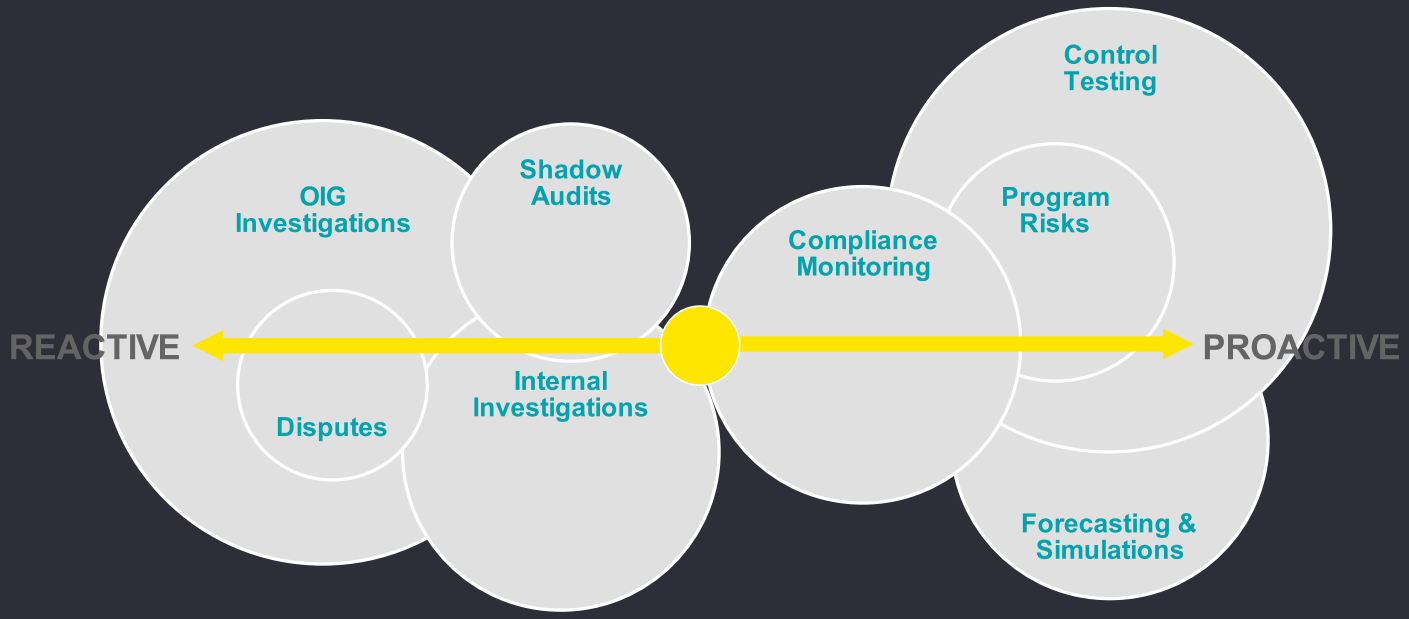


Respond to Fraud Risks
Defining data analytics

Data analytics applies techniques and technologies to distill relevant insights from large volumes of data for contextualized decisions making.



Respond to Fraud Risks
Applications of data analytics



Respond to Fraud Risks
Example analytic techniques

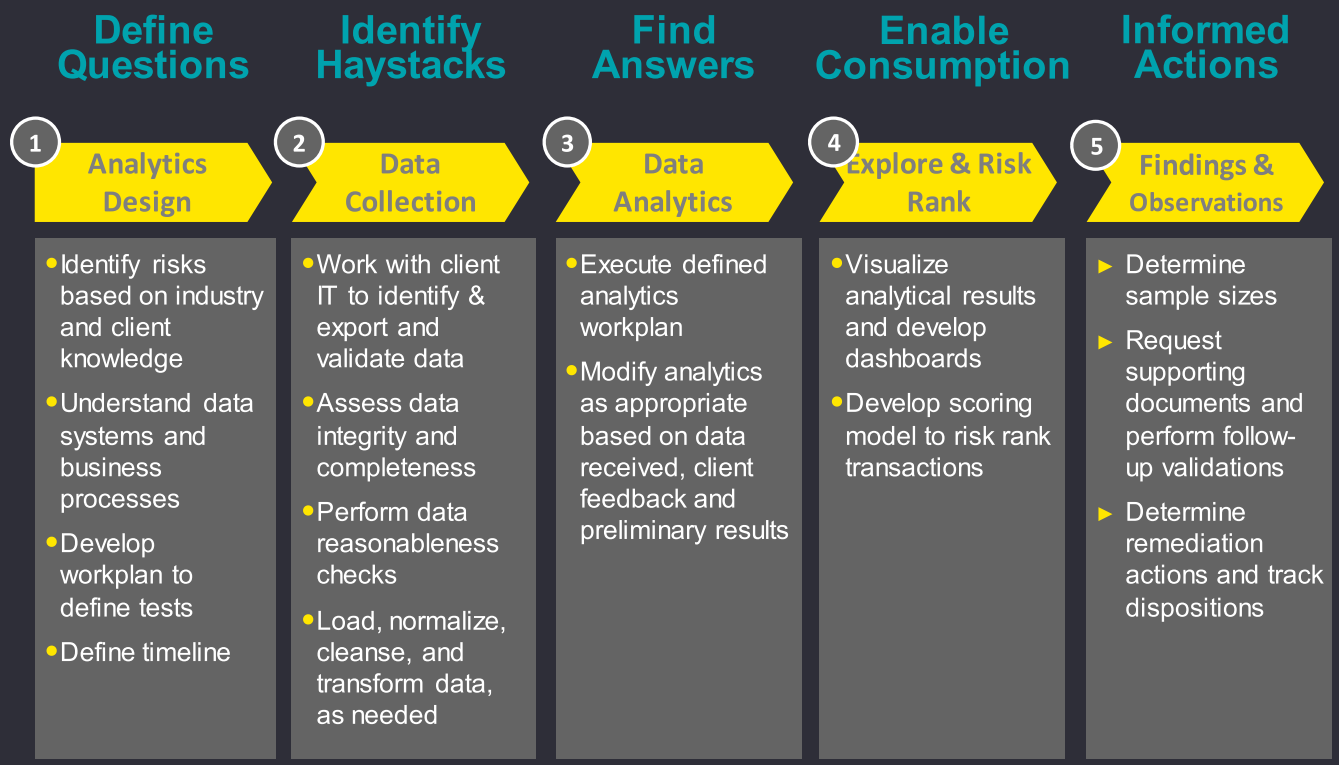
Fraud Analytics

Rule-based analytics	Anomaly detection analytics	Predictive analytics	Network/link analytics	Text analytics
				
Known patterns	Unknown patterns	Complex patterns	Linked patterns	Text patterns
Common fraud		Criminal fraud		Organized fraud

Respond to Fraud Risks
Data analytics challenges and considerations

- IT Security Compliance
  - Can we safely secure sensitive data types?
  - Can we send data to contractors off-site?
  - Is the contractor's data management policy compliant
- Cyber awareness training
  - Required for each member of the contracting team
- Nondisclosures
  - Required for each member of the contracting team
- Privacy Act (PII)
  - Is the data considered sensitive and who can access it?
- Data
  - Where is the data(does it exist)?
  - Who owns it and how can we get it?
  - Is it right (complete and valid)?

Respond to Fraud Risks
Systematic methodology

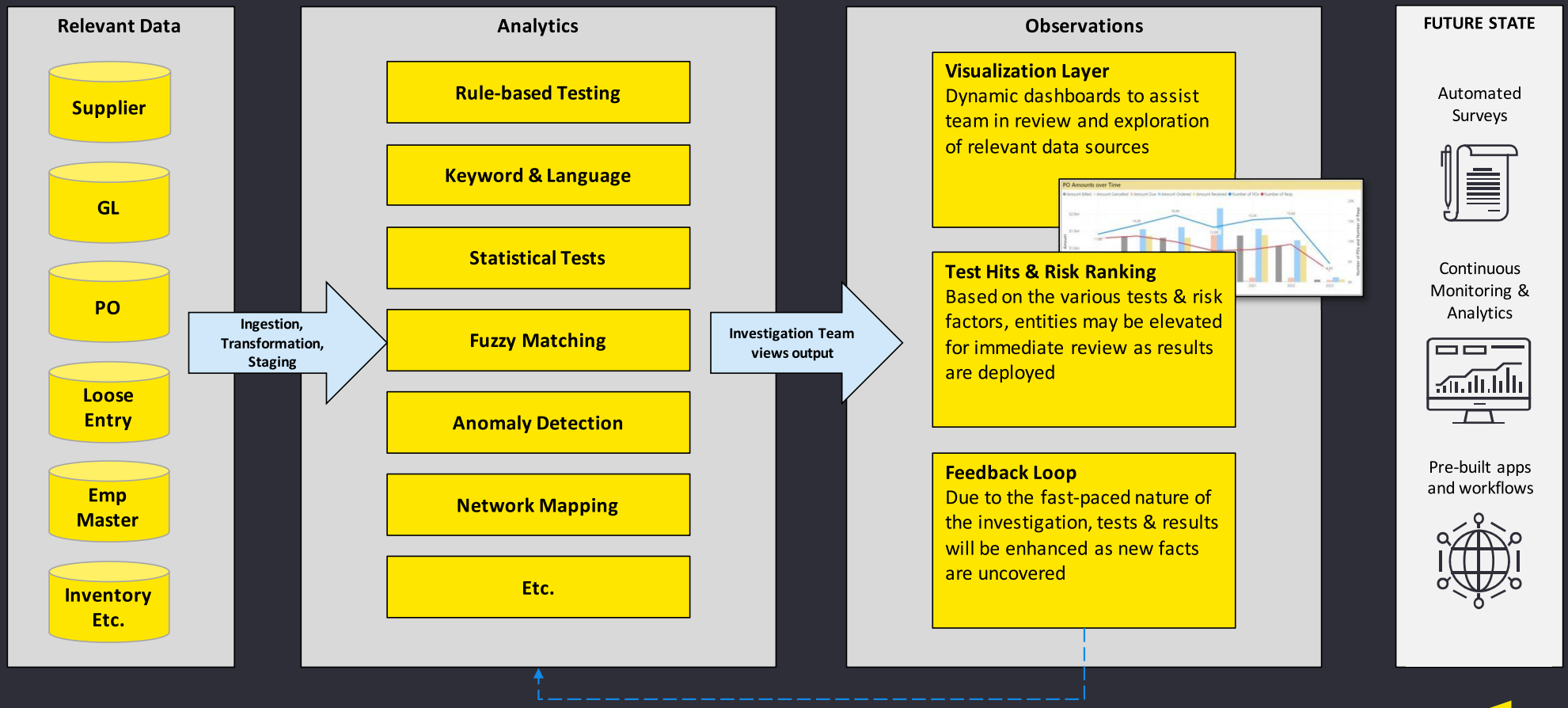


Respond to Fraud Risks

Enhanced controls and processes

Collaborate with internal audit to document the risk assessment results and monitor control testing related to key risks	• Internal control testing should provide a continuous source of data related to the effectiveness of key anti-fraud controls
Develop role-based training and evaluate its effectiveness	• Training should be tailored to the organization and the roles most at risk
Reassess risks as your program and environment change	• Fraud is an ever-evolving threat and must be continuously monitored
Communicate key findings to leadership	• Make leadership aware of the highest priority fraud risks and what the agency is doing to address them. Most organizations hesitate to share fraud risks because they fear increased scrutiny, which leads to increased risk of the events occurring.

Respond to Fraud Risks
Case Study: Procurement fraud investigation



Respond to Fraud Risks
Anti-fraud Resources

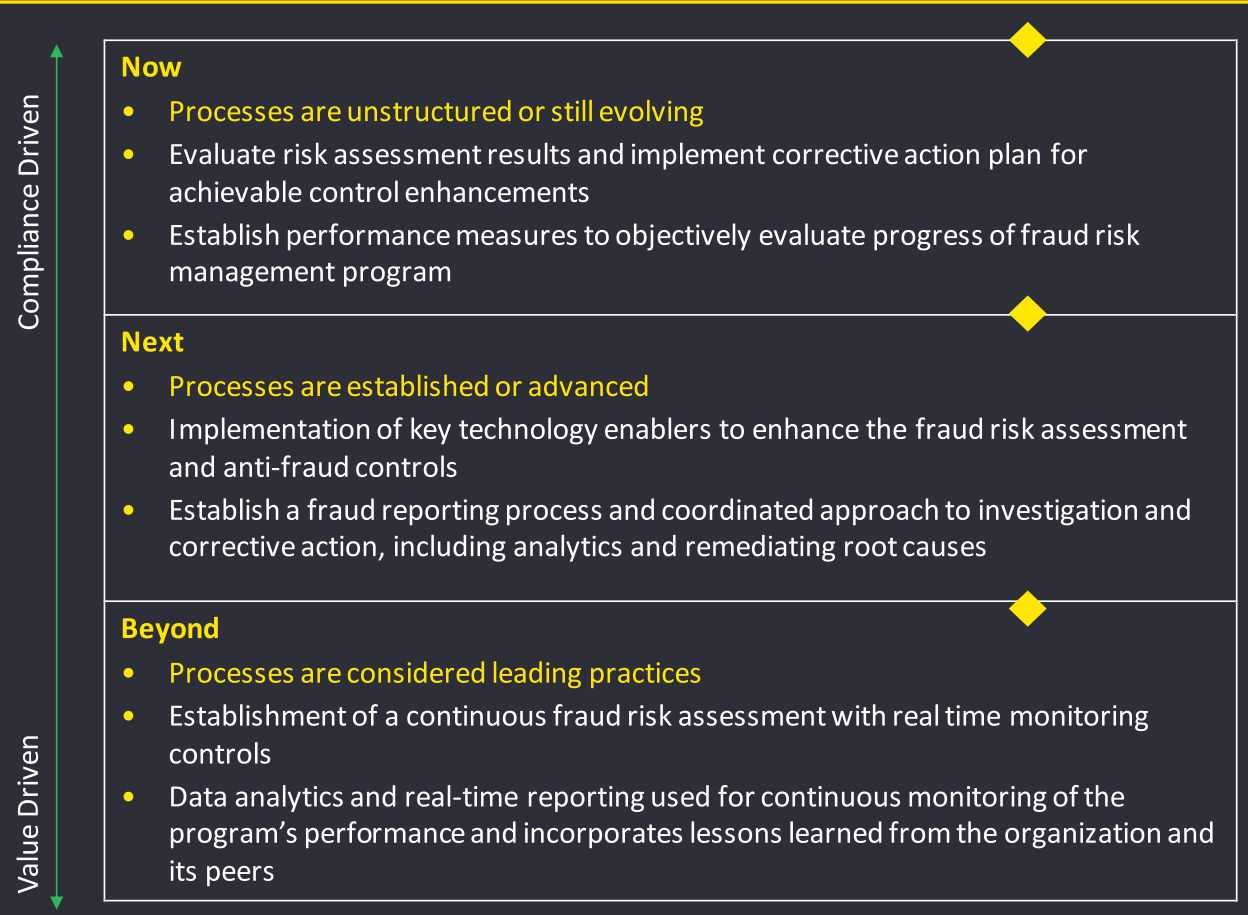
- Program Integrity: The Antifraud Playbook
- Government Accountability Office, Interactive Antifraud Resource
- Government Accountability Office, Fraud Framework
- Pandemic Response Accountability Committee, Lesson Learned
- AGA Fraud Prevention Toolkit
- Dept. of the Treasury, Do Not Pay
- Dept. of the Treasury, Payment Integrity Center of Excellence
- COSO Fraud Risk Management Guide
- ACFE Toolkit

Evaluate & Adapt

5 minutes

Building a better working world

Evaluate & Adapt



Questions and Wrap-up

5 minutes

Building a better working world