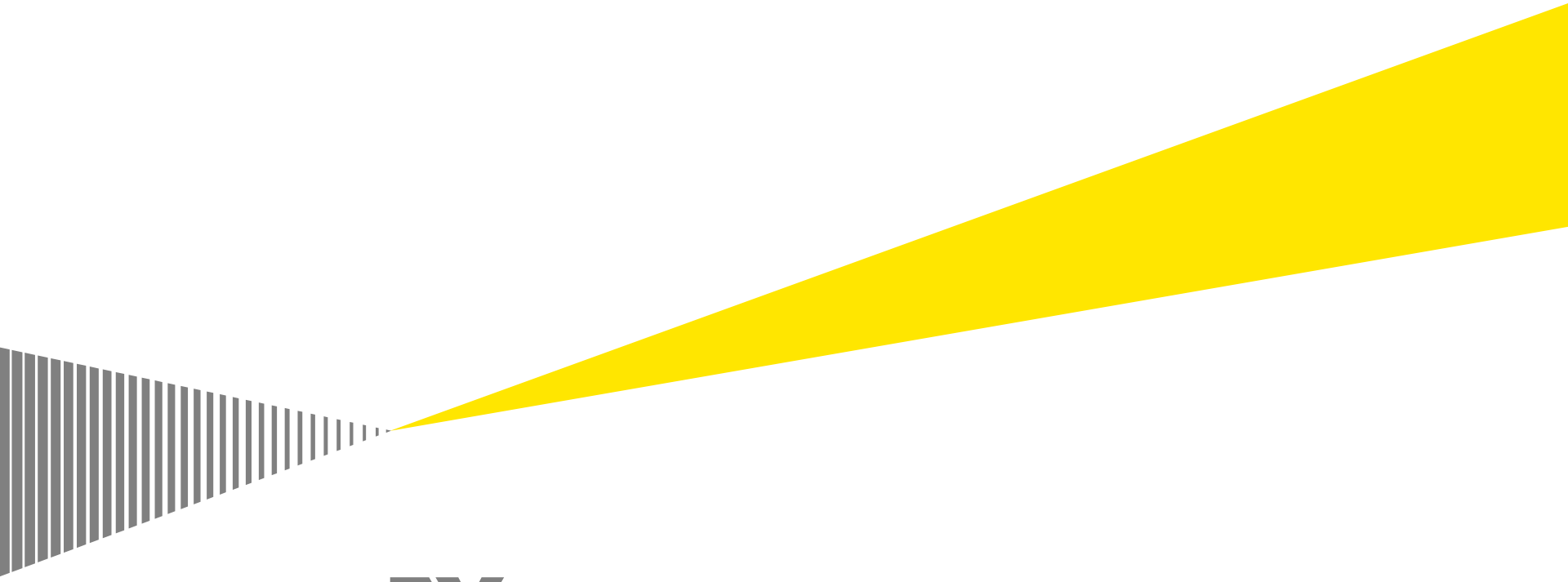
Implementing COSO's New Fraud Risk Management Guidelines



EY
Building a better working world

Fraud risk management is much more than a mere fraud risk assessment…

The responsibility for managing fraud risk falls on everyone:

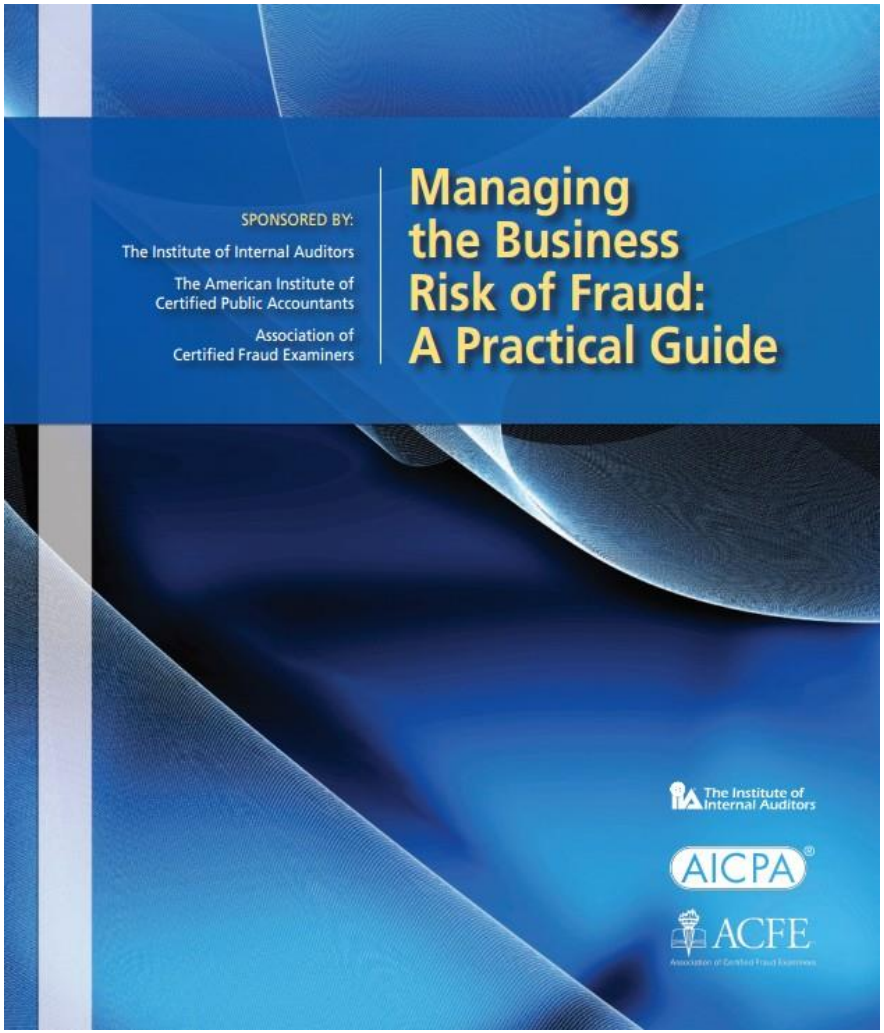
- *"The board of directors, and top management and personnel at all levels of the organization — including every level of management, staff, and internal auditors — have responsibility for managing fraud risk."*

Fraud deterrence is achieved when the organization:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Includes a thorough fraud risk assessment periodically
- Designs, implements, and maintains preventive and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

Source: 2016 COSO Fraud Risk Management Guidelines

2008: First major attempt to increase fraud risk management and fraud risk assessments

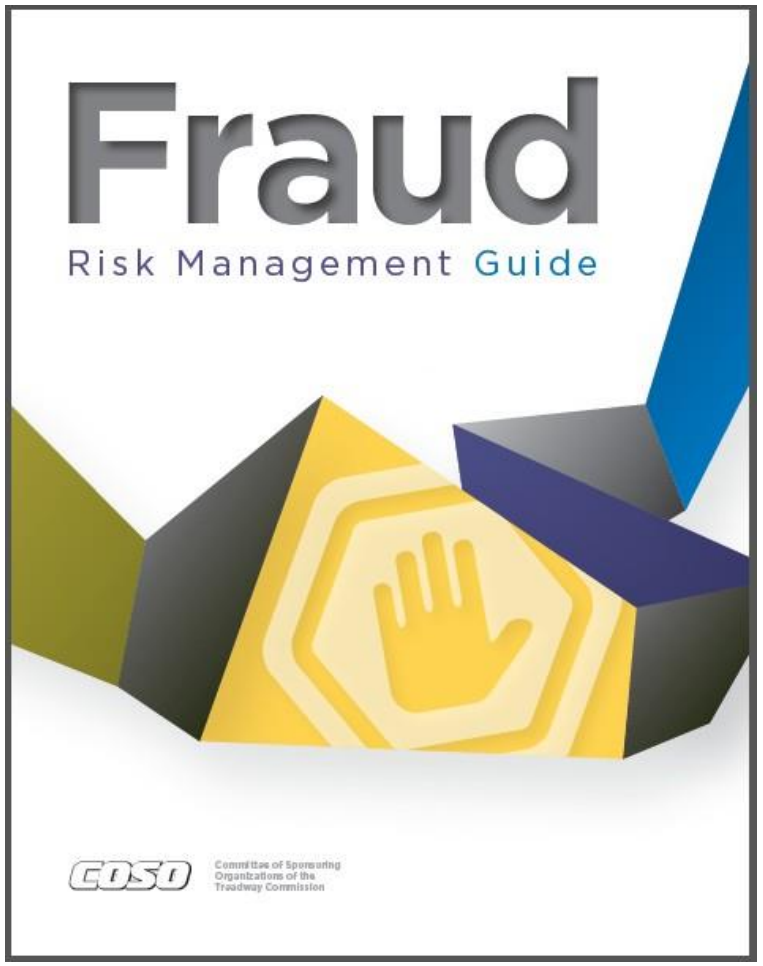


IIA, ACFE, AICPA Sponsors

- Fraud Risk Governance
- Fraud Risk Assessment
- Fraud Prevention
- Fraud Detection
- Fraud Investigation and Corrective Action

2016 COSO Fraud Risk Management Guidelines

1) Establishment of a Fraud Risk Management Program
2) Performs comprehensive fraud risk assessments
3) Selects, develops and deploys preventative and detective fraud control activities
4) Investigation program
5) Ongoing evaluations and corrective action of the overall program



Source: 2016 COSO Fraud Risk Management Guidelines

Summary of Fraud Risk Management Components and Principles

Control Environment

Principle 1 The organization establishes and communicates a Fraud Risk Management Program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

Risk Assessment

Principle 2 The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.

Control Activities

Principle 3 The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.

Information & Communication

Principle 4 The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.

Monitoring Activities

Principle 5 The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates Fraud Risk Management Program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.

Source: 2016 COSO Fraud Risk Management Guidelines

What do the COSO Fraud Risk Management Guidelines (FRMG) mean for my organization?

COSO ERM Organization

- A fraud risk assessment no longer covers the expectation of Principle 8 of COSO – ERM Framework
- A **formal** fraud risk management program is the expectation.
- Internal auditors are expected to assess internal anti-fraud processes and controls against the FRMG
- External Auditors can assess the entity's implementation of Principle 8 of the COSO ERM Framework using this guide.

Non-COSO Organization

- Non-COSO organizations will be unable to claim that sufficient guidance or information anti-fraud programs, controls, processes and systems was not available.
- Fraud loss litigation, such as shareholder suits, could point to the COSO FRM Guidelines and place more responsibility for the loss on management and the lack of an effective anti-fraud program.

Principle 1 - Fraud Risk Governance

Principle 1 - Fraud Risk Governance

Board and Senior Management:

- Makes an organizational commitment to fraud risk management.
- Supports fraud risk governance.
- Establishes a comprehensive fraud risk management policy.
- Establishes fraud governance roles and responsibilities throughout the organization.
- Documents the fraud risk management program.
- Communicates fraud risk management at all organization levels.

Source: 2016 COSO Fraud Risk Management Guidelines

A ***Documented*** and ***Formal*** fraud risk management program

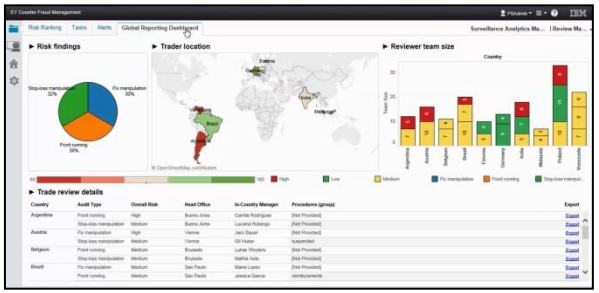
1. A stand-alone comprehensive document addressing in detail all aspects of fraud control activities.
2. Development of a brief strategy outline emphasizing the attributes of fraud control activities with design and specifics left to the responsible business functions.
3. Providing defined, proactive processes and control activities to deter, prevent, and detect fraud AND the individuals who will execute the activities.
4. Providing a strategy for proactively using data analysis
5. Providing a compilation of plans developed by divisions or subsidiaries

Source: 2016 COSO Fraud Risk Management Guidelines

Analytics considerations
Principles 1 through 5: Aligned with Governance

Control Environment

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
1. The organization demonstrates a commitment to integrity and ethical values	**1. The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.**	• Executive reporting • Interactive dashboards • Targeted analysis around metrics, compliance and ratios
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
4. The organization demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		



Principle 2 – Fraud Risk Assessment

Principle 2 – Fraud Risk Assessment

- Involves the appropriate level of management
- Includes entity, subsidiary, division, operating unit and functional levels
- Analyzes internal and external factors
- Considers various types of fraud
- Specifically considers the risk of management override of controls
- Estimates the likelihood and significance of risks identified
- Assess personnel or departments involved and all aspects of the fraud triangle
- Identifies existing fraud control activities and assesses their effectiveness
- Determines how to respond to risks
- Uses data analytics techniques for fraud risk assessment and fraud risk responses
- Performs periodic risk assessments and assess changes to fraud risk
- Documents the risk assessment

Source: 2016 COSO Fraud Risk Management Guidelines

Analytics considerations
Principles 6 through 9: Aligned with Fraud Risk Assessment

Risk Assessment

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.	**2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.**	• Surveys & heat maps • Media scans and external sources such as industry news • Complaints database
9. The organization identifies and assesses changes that could significantly impact the system of internal control.		

Principle 3 - Fraud Control Activities

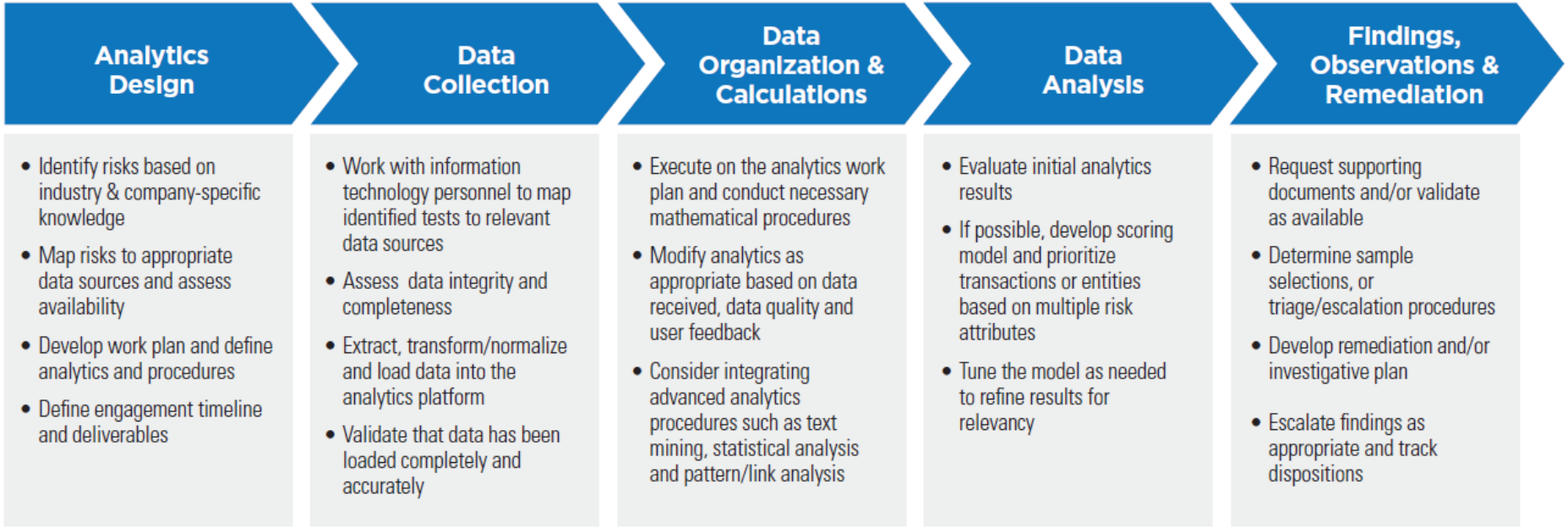
Principle 3 – Fraud Control Activities

- Promotes fraud deterrence through **preventive** and **detective** control activities
- Integrates with the fraud risk assessment
- Considers organization-specific factors and relevant business processes
- Considers the application of control activities to different levels of the organization
- Utilizes a combination of fraud control activities
- Considers management override of controls
- Uses ***proactive*** data analytics procedures
- Deploys control activities through policies and procedures

Source: 2016 COSO Fraud Risk Management Guidelines

A comprehensive and methodical data analytics process is the key

Figure 12. Example of a Data Analytics Framework



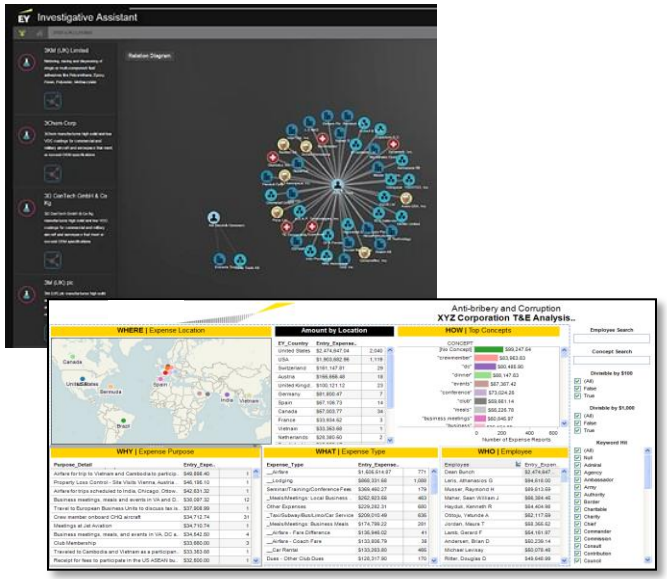
Source: 2016 COSO Fraud Risk Management Guidelines

Analytics considerations

Principles 10 through 12: Aligned with Fraud Control Activities

Control Activities

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.**	• ABaC analytics • P2P, O2C, T&E, CRM analysis • General ledger transaction analysis
11. The organization selects and develops general control activities over technology to support the achievement of objectives.		
12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.		



http://www.ey.com/PZ/en/Home/EYCounterFraudManagementDemo

Frequent compliance analytics risk areas, particularly in emerging markets

Meals & Entertainment	Marketing & Events	CRM and Sales
Information Security/Insider Threat	Employee Payroll	Sales, Distributor & Margin Analysis
Vendor Payments / AP	Capital Projects	Accounting Reserves
Inventory	3rd Party Due Diligence & Watchlist, Shell Companies	Charity & Donations

Emerging monitoring activities may include...

Social Media Monitoring	Advanced Email Monitoring	Mobil Devices

Big data techniques to counter fraud

- Multiple data sources – structured and unstructured
- Data visualization
- Text analytics
- Payment/transaction risk scoring
- Predictive modeling – technology assisted monitoring
- Case management, issue coding and built in workflow
- Flexible deployment models

Utilizing data visualization to do more

Plan and build tests for:

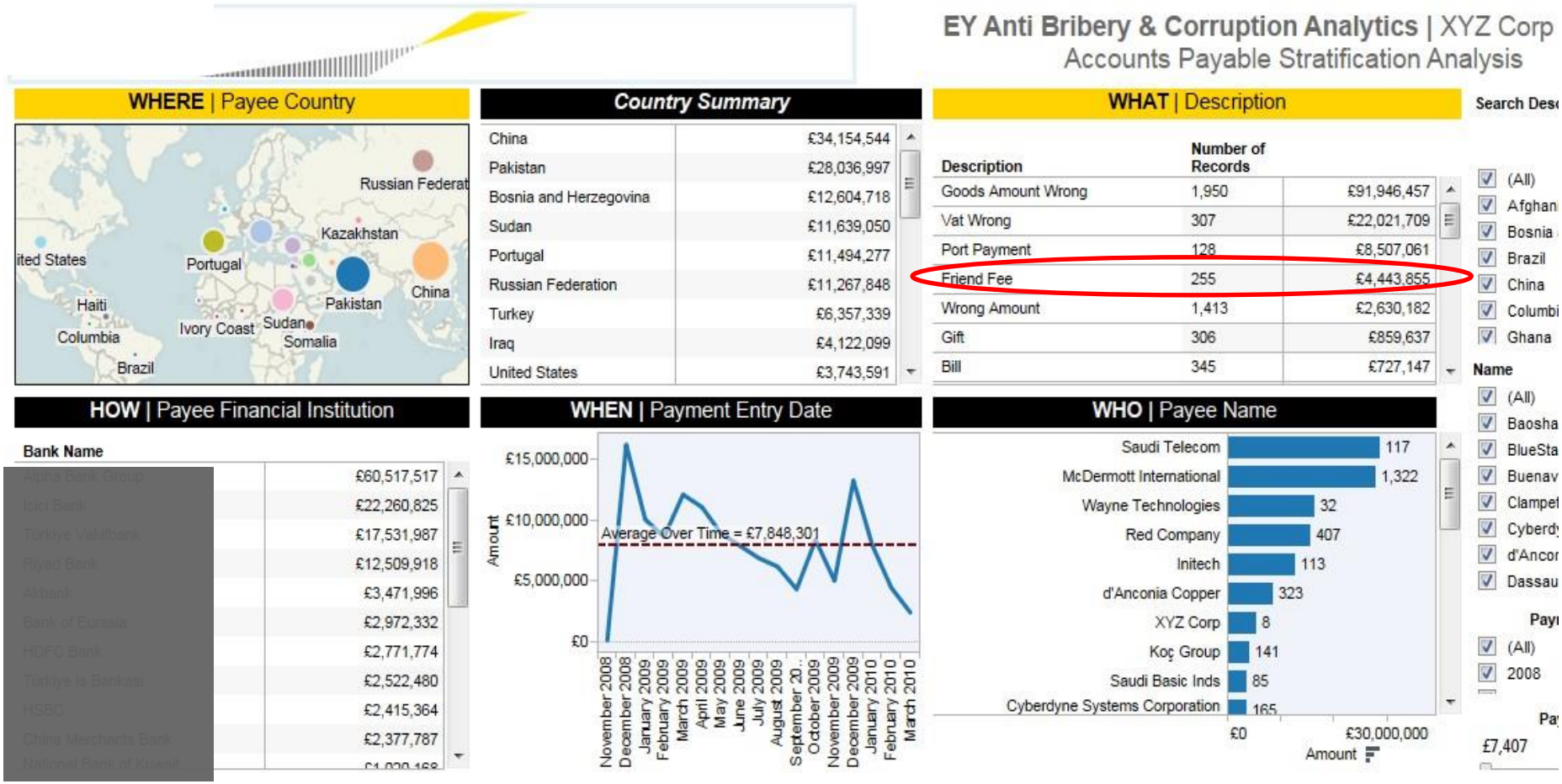
- ✓ Payment risk scoring
- ✓ Vendor risk scoring
- ✓ High risk transactions
- ✓ Revenue recognition or sales commissions
- ✓ Conflicts of interests

Additional tests for enhanced reviews:

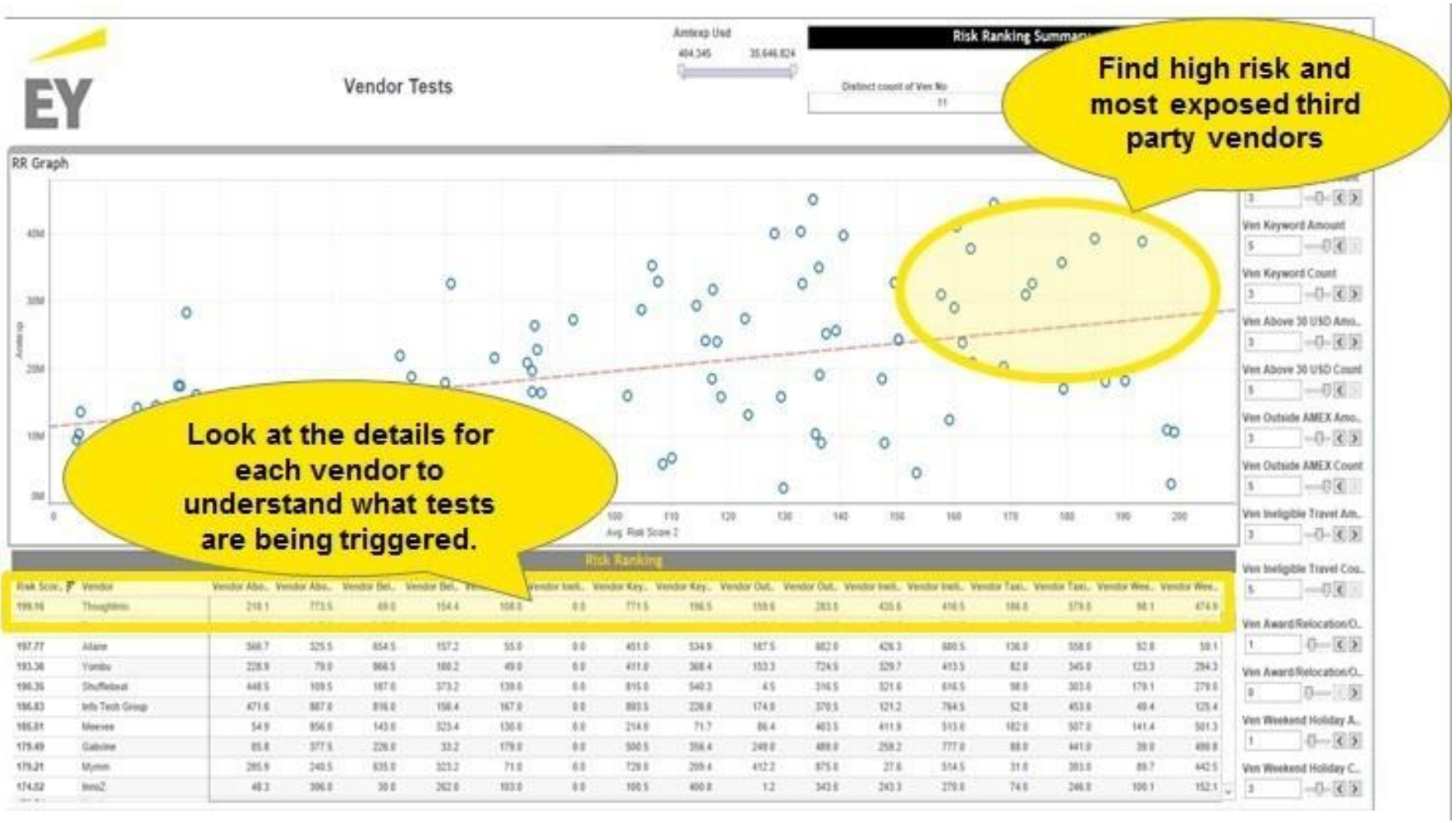
- ✓ Inventory management
- ✓ Salaries & payroll
- ✓ Employee travel & entertainment
- ✓ FCPA/UKBA (corruption risks)
- ✓ Selected compliance topics

Data visualization: Accounts payable monitoring

High risk payment descriptions

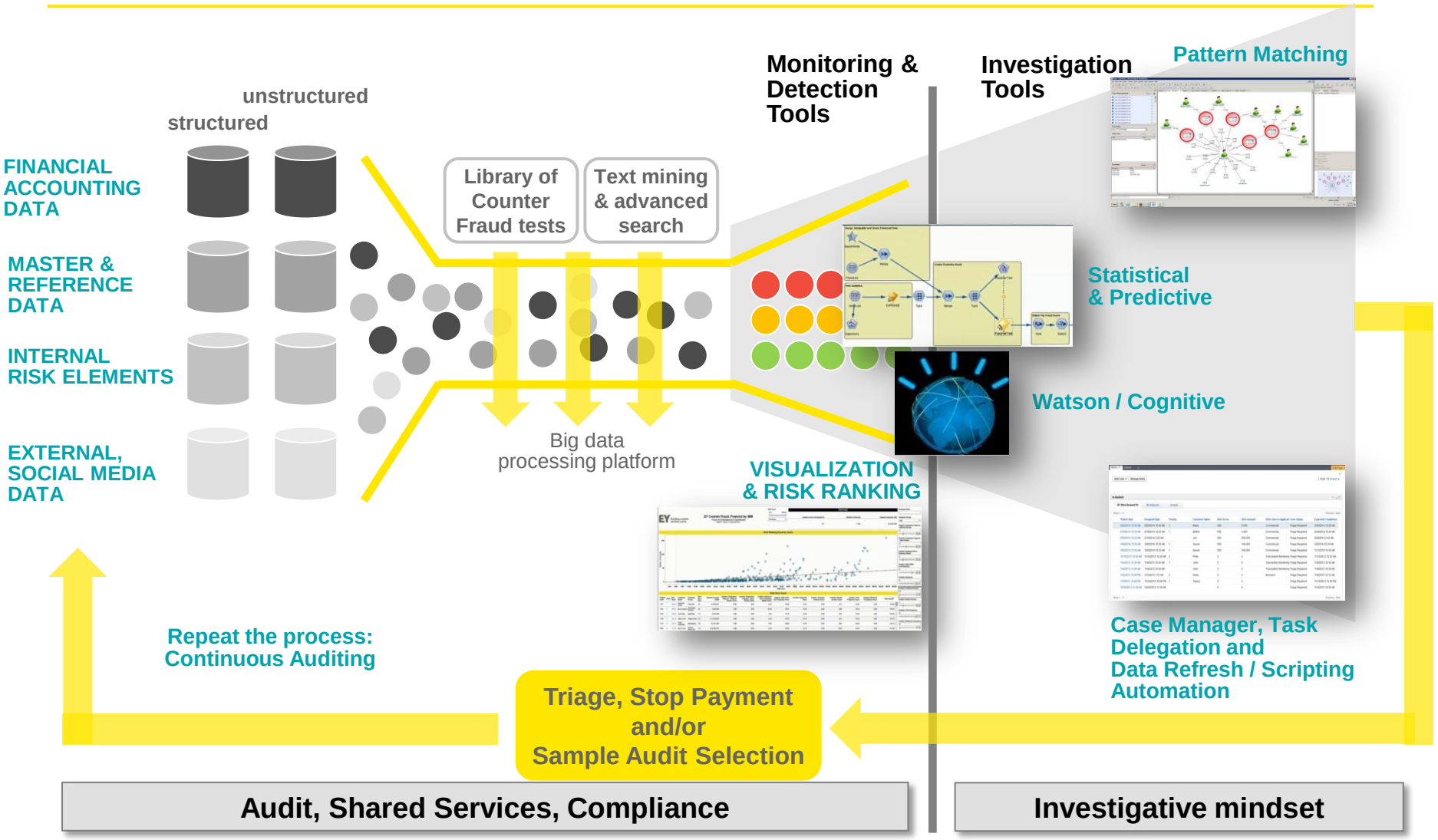


Utilizing transaction risk scoring to do more



Forensic data analytics framework

An integrated, platform – from a work flow and monitoring perspective



Principle 4 - Fraud Investigation and Corrective Action

Why is a formal investigation program necessary?

- Increasing number of poorly performed investigations
- Frauds and fraudsters missed,
- Root causes not obtained and internal controls not improved,
- Legal and human resource implications,
- Poor interviewing skills and increased liabilities,
- Lack of dedicated and experienced forensic or investigative skill sets,
- Inadequate technological resources,
- Lack of routine and repetitive investigation training
- Inconsistent or non-existent corrective action
- Poor investigation tracking and reporting mechanisms

Principle 4 - Fraud Investigation and Corrective Action

- Establishes fraud investigation and response protocols
  - Confidentiality, urgency, evidence preservation, legal protections, forensic support, investigation protocols, reporting process, root cause and mitigating controls, etc.
- Conducts investigations
- Communicates investigation results
- Takes corrective action
- Evaluates investigation performance

Source: 2016 COSO Fraud Risk Management Guidelines

Monitoring investigation performance metrics

- Resolution time
- Investigation costs
- Repeat incidents
- Incident location (business unit, operational area or geography)
- Value of losses recovered and future losses prevented
- Corrective actions
  - Internal control remediation, business process remediation, disciplinary action, training, insurance claims, extended investigations, civil actions, criminal referrals
  - **Corrective actions for fraud related incidents is an evaluation component within the Federal Sentencing Guidelines

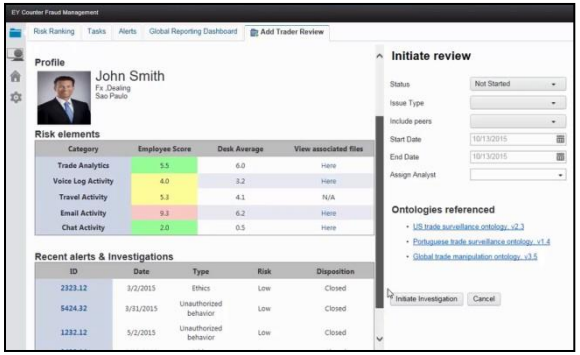
Source: 2016 COSO Fraud Risk Management Guidelines

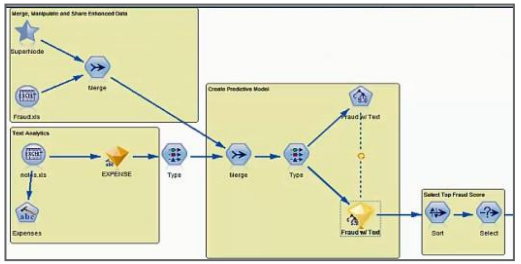
Analytics considerations

Principles 13 through 15: Aligned with Investigative Activities

Information & Communication

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
13. The organization obtains or generates and uses relevant, quality information to support the functioning of other components of internal control.	**4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.**	• Case management • Escalation and triage • Review workflow management
14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.		





Principle 5 - Fraud Risk Management Monitoring Activities

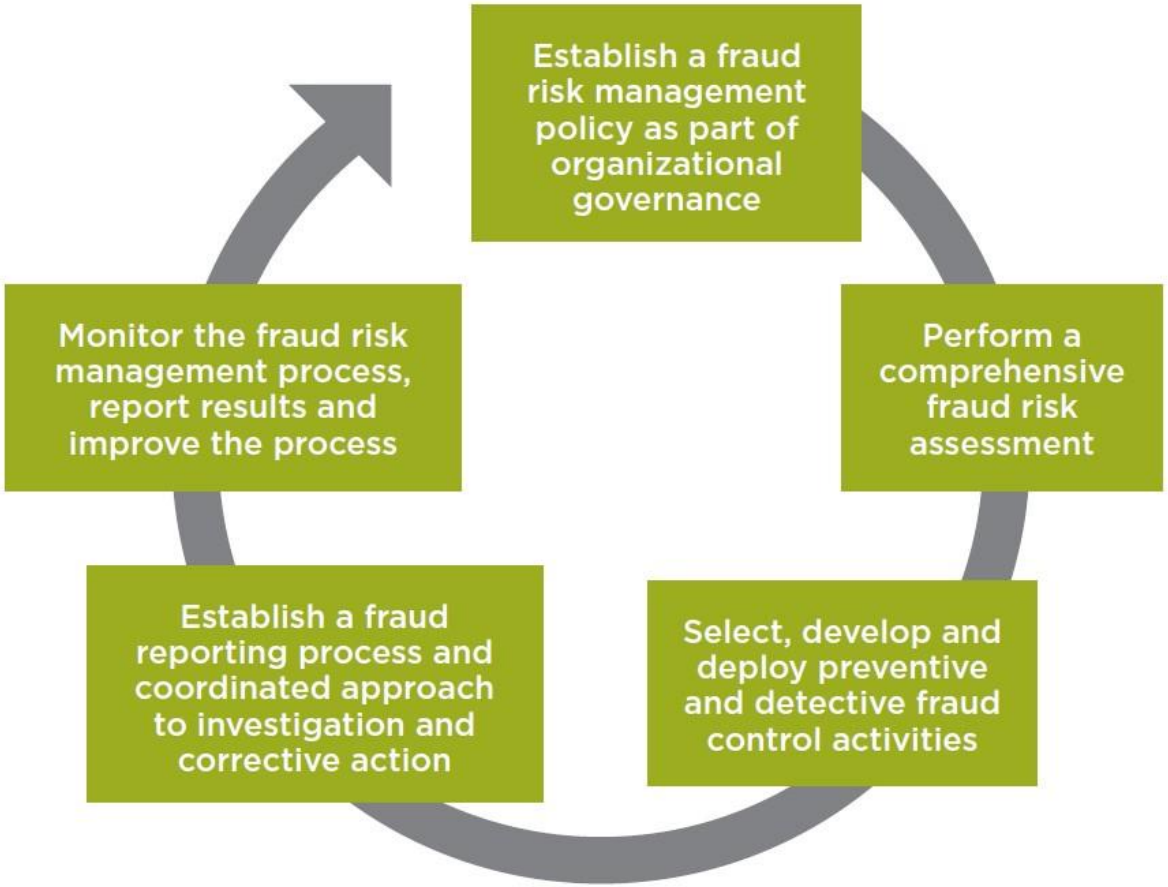
Principle 5 - Fraud Risk Management Monitoring Activities

- Considers a mix of ongoing and separate evaluations
- Considers factors for setting the scope and frequency of evaluations
- Establishes appropriate measurement criteria
- Considers known fraud schemes and new fraud cases
- Evaluate, communicates and remediates deficiencies

Source: 2016 COSO Fraud Risk Management Guidelines

Fraud risk management monitoring brings the process full circle and becomes cyclical

Figure 1. Ongoing, Comprehensive Fraud Risk Management Process

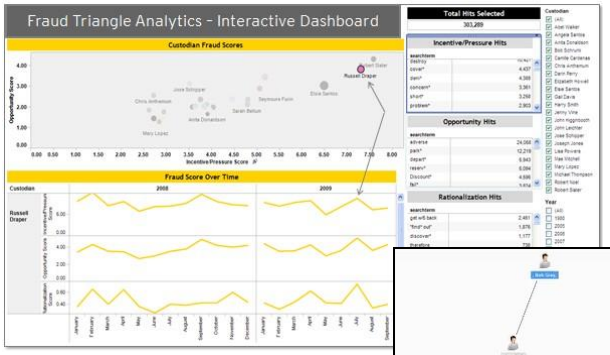


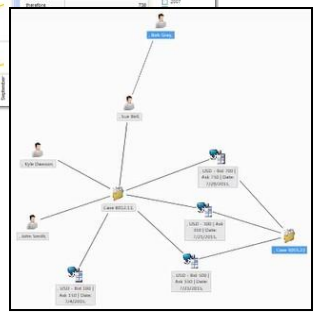
Source: 2016 COSO Fraud Risk Management Guidelines

Analytics considerations
Principles 16 & 17: Aligned with Monitoring Activities

Monitoring Activities

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
16. The organization selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.**	• Investigative procedures • Deep dive analysis • Email and communications review
17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		





Key takeaways, action items and next steps

- Determine your organization's adherence to COSO ERM Framework, whether formal, informal or not at all
- Identify and formalize all anti-fraud and investigation activities under the umbrella of a formal and documented fraud risk management program
- Identify the appropriate sponsor and/or process owner(s)
- Conduct an assessment to identify gaps, weaknesses and duplicative or ineffective anti-fraud efforts
- Develop/enhance and deploy comprehensive preventative and detective data analytics capabilities
- Integrate the fraud risk management components throughout the organization

Thank you

EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.
Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

Ernst & Young LLP, an equal opportunity employer, values the diversity of our work force and the knowledge of our people.

SCORE no. XX0000

1603-1886034
ED none
EY is committed to reducing its impact on the environment. This document was printed using recycled paper and vegetable-based ink.

ey.com