Institute of Internal Auditors
Seattle Chapter
PwC Update on fraud management trends & opportunities
Presenting to you today

Frank Badalamenti
Principal
(646) 818-7158
frank.badalamenti@pwc.com

David Fapohunda
Managing Director
(646) 471-3144
david.fapohunda@pwc.com
Enhanced fraud operating model for complex fraud environment
Our point of view – Balanced fraud risk management oversight

Leading fraud management principles focused on fraud risk factors

### Key risk factors shaping fraud management

<table>
<thead>
<tr>
<th>Lines of Business</th>
<th>Products</th>
<th>Leading principles</th>
</tr>
</thead>
</table>
| Organization & People | • Accountability, roles and responsibilities across the three lines of defense are clear  
• Appropriate skill sets and staffing model to meet objectives |
| Governance | • Managing the balance between all ‘shades’ of the lens  
• Enabling functions across all 3 Lines of Defense to meet goals |
| Operations | • Creating efficiencies to reduce operating costs  
• Layering processes to prevent, detect and respond |
| Technology & Tools | • Utilizing layered and orchestrated preventative, detective, and responsive customer engagement solutions |
| Data & Analytics | • Enabling access to real-time or near-real-time data  
• Enhancing decision making with deep learning and AI |
| Customer | • Balancing customer friction with customer security  
• Creating lifetime value and customer trust |
# Fraud management framework

End-to-end framework for managing fraud across lines of defense

## PwC Fraud Governance Framework

<table>
<thead>
<tr>
<th>1st Line of Defense (LOD)</th>
<th>Functions</th>
<th>Data &amp; Technology</th>
<th>People</th>
<th>Data</th>
<th>Fraud Lifecycle</th>
<th>2nd LOD</th>
<th>3rd LOD</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Multi-Factor Authentication</td>
<td>Surveillance/ Monitoring</td>
<td>-</td>
<td>-</td>
<td>External Fraud</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>People</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Data</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Fraud Lifecycle</td>
<td>Prevent</td>
<td>Detect</td>
<td>Investigate &amp; RemEDIATE</td>
<td>Mine &amp; Measure</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>

## Fraud Lifecycle

- **Prevent**
  - Employee HR data
  - Entitlements
  - Vendor master
  - Customer master

- **Detect**
  - Transactional activity
  - Voice recordings
  - Compensation data
  - Procurement events
  - Accessed data (logs)
  - Physical access logs
  - Email
  - Fraud alert/case data

- **Investigate & RemEDIATE**
  - Customer master
  - Historical data
  - Email
  - Voice recordings
  - Account & Transaction Data (Wire, ACH, Check, Card, Trades, BillPay)
  - Non-monetary transactions
  - Online activity
  - External data feeds (blacklists, non-monetary data)
  - Internal negative lists

## Resources

- **Resource Capacity**
  - Resource Capacity
  - Resource Capacity
  - Resource Capacity
  - Resource Capacity
  - Resource Capacity
  - Resource Capacity
# PwC PoV on fraud risk management 2nd LOD structure

## Leading practices for the 2nd LoD fraud management functional teams

<table>
<thead>
<tr>
<th>Head of fraud risk management</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Governance and Advisory</strong></td>
</tr>
<tr>
<td>Operating Committee &amp; Board Coordination</td>
</tr>
<tr>
<td>Fraud Regulatory &amp; Audit Interface</td>
</tr>
<tr>
<td>Enterprise Fraud Training &amp; Education</td>
</tr>
<tr>
<td>Client Experience Oversight</td>
</tr>
<tr>
<td>Fraud Model Governance Risk Approval</td>
</tr>
</tbody>
</table>

*PwC | Institute of internal auditors*
Fraud risk management – Governance interaction model
Illustrative model for fraud risk governance
Fraud operating model – PwC design principles

We leverage our leading practice design principles to assess and implement operating models bespoke to our clients’ business and optimized to manage across fraud risk factors.

<table>
<thead>
<tr>
<th>Design Principles for Fraud Operating Model</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Collaboration &amp; Sharing</strong></td>
</tr>
<tr>
<td>Enhance collaboration and sharing</td>
</tr>
<tr>
<td>Develop a coordinated fraud strategy to</td>
</tr>
<tr>
<td>promote collaboration and intelligence</td>
</tr>
<tr>
<td>sharing across fraud prevention and</td>
</tr>
<tr>
<td>detection functions</td>
</tr>
<tr>
<td>1</td>
</tr>
<tr>
<td><strong>Roles &amp; Responsibilities</strong></td>
</tr>
<tr>
<td>Define clear roles &amp; responsibilities</td>
</tr>
<tr>
<td>Consolidate fraud functions, where</td>
</tr>
<tr>
<td>possible, and formalize roles and</td>
</tr>
<tr>
<td>responsibilities (and interaction model)</td>
</tr>
<tr>
<td>across the 3 Lines of Defense.</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td><strong>Efficiency</strong></td>
</tr>
<tr>
<td>Assess levers that can increase efficiency</td>
</tr>
<tr>
<td>Reduce duplication of roles, map</td>
</tr>
<tr>
<td>processes to identify process</td>
</tr>
<tr>
<td>inefficiencies and identify opportunities</td>
</tr>
<tr>
<td>to apply automation and technology to make</td>
</tr>
<tr>
<td>efficiency gains</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td><strong>Execution Excellence</strong></td>
</tr>
<tr>
<td>Set up for effective execution</td>
</tr>
<tr>
<td>Ensure that fraud teams are ‘set up for</td>
</tr>
<tr>
<td>success’ (systems, processes and</td>
</tr>
<tr>
<td>training); and KPI’s are established to</td>
</tr>
<tr>
<td>monitor and course correct performance</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td><strong>Connected with Business &amp; Customer</strong></td>
</tr>
<tr>
<td>Aligned to business</td>
</tr>
<tr>
<td>Ensure that fraud team goals are aligned</td>
</tr>
<tr>
<td>with business growth goals (e.g., new</td>
</tr>
<tr>
<td>product introduction) and customer</td>
</tr>
<tr>
<td>experience goals. Risk appetite alignment</td>
</tr>
<tr>
<td>is critical.</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td><strong>Built for the Future</strong></td>
</tr>
<tr>
<td>Scalable structure</td>
</tr>
<tr>
<td>Build a flexible and scalable framework to</td>
</tr>
<tr>
<td>adapt to threats and industry trends, one</td>
</tr>
<tr>
<td>of which will be Financial Crimes</td>
</tr>
<tr>
<td>convergence</td>
</tr>
<tr>
<td>6</td>
</tr>
</tbody>
</table>
Reflection question 1

Does your organization have designated fraud management specific roles in both the 1st line and the 2nd line of defense?

A. Yes, we have separate and distinct fraud management roles as part of the 1st line AND 2nd line
B. No, all fraud management roles reside in the 1st line only
C. No, all fraud management roles reside in the 2nd line only
D. None of the above, there are no fraud management specific roles in the organization. Fraud management is assumed under broader roles that include additional responsibilities.
Reflection question 2

In which of the following fraud lifecycle areas has your institution made the most investments or control/process enhancements over the past 1 - 2 years?

A. Prevention
B. Detection
C. Investigation & Remediation
D. Mine & Measure (e.g., defect analysis & feedback loops)
Fraud risk assessment – Themes raised across the industry
## Risk & themes in fraud risk assessments during COVID

<table>
<thead>
<tr>
<th>Risks</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase in email schemes/scams</td>
<td>Elevated occurrence of corporate payment disbursement fraud via unauthorized payment request, unauthorized payment account modification either by business email compromise (BEC), vendor compromise and employee collusion</td>
</tr>
<tr>
<td>Account Takeover targeting reward and stored value cards</td>
<td>External and internal bad actors have changed tactics due to reduced cash based transactions. Stored value cards (gift cards, shopping cards) have increasingly become attractive</td>
</tr>
<tr>
<td>Extended work from home risks</td>
<td>Process for existing full-time employees new hire, seasonal hire and contractor roles may need to be reviewed to understand impact of risk acceptances, unaddressed gaps and vulnerability hunting</td>
</tr>
</tbody>
</table>
## Risk & themes in fraud risk assessments during COVID (continued)

<table>
<thead>
<tr>
<th>Themes</th>
<th>Considerations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-retail fraud program</td>
<td>Development of fraud identification, escalation, measurement, and processes within corporate functions</td>
</tr>
<tr>
<td>Aggregated fraud reporting</td>
<td>Siloed fraud reporting, consistency and depth affecting ability to report enterprise fraud threats to business leaders and board</td>
</tr>
<tr>
<td>New process and initiatives fraud assessment</td>
<td>Enhancement of new product and new process governance process to have anti-fraud by design as a principle throughout the change lifecycle</td>
</tr>
<tr>
<td>Fraud model governance oversight</td>
<td>Fraud models have becoming more sophisticated and are making more autonomous decisions on behalf of organizations. Due to COVID these models are also adversely being affected due to transaction patterns that were never seen in model training data sets</td>
</tr>
</tbody>
</table>
Reflection question 3

Which of the following thematic trends are leading to the biggest change in how you are assessing or evaluating fraud risk?

A. Increase in email scams and business email compromise schemes
B. Increase in employees working from home vs. the office
C. Shift of sales volume from in-store/in-branch to mobile and web
D. Launch of new products and services
Reflection question 4

Which of these functions takes the most prominent role in conducting a periodic fraud risk assessment in your organization?

A. 2nd Line Risk Management
B. Investigations Unit/SIU
C. Internal Audit
D. 1st Line Business Owners
E. None of the Above
Using enhanced analytics and fraud testing
We developed a high-level strategy for the use of data analytics to combat fraud, and a framework with the objective to create analytic-based solutions designed to create operational efficiency, augmented fraud detection, and reduce risk.
In assessing an organization’s Fraud Technology & Analytics architecture, we evaluate solutions in use across the fraud lifecycle. This is a critical component of fraud management, and starts with understanding the evolving vendor landscape. Below are some vendors for each stage of the fraud lifecycle (Note: this is not an exhaustive list).

<table>
<thead>
<tr>
<th>Digital Identity Verification</th>
<th>Authentication</th>
<th>Surveillance &amp; Detection</th>
<th>Referral Tool</th>
<th>Analysis &amp; Investigation</th>
<th>Journey Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use of internal and third party data to perform due diligence on potential clients during the onboarding process. • TransUnion, Experian • Simility • Emailage • ProvePayfone</td>
<td>Authenticators such as voice biometrics, OTP or dynamic KBAs are combined to determine whether someone is who he/she is declaring to be. • TrustStamp • Onfido • ThreatMetrix • PinDrop • Transmit Security</td>
<td>Discover emerging patterns of fraud via machine learning or advanced analytics. • Actimize • SAS • FICO Falcon • Feedzai • Featurespace • DataVisor</td>
<td>Allow employees and third parties to escalate known or suspected fraudulent activity to investigations units. • Internal Development • Actimize • Archer • IBM BPM</td>
<td>Perform root cause analysis, assist with ongoing and past investigations and uncover new fraud schemes. • SAS • Splunk • RSA SilverTail</td>
<td>Understand pain points in the customer journey and capture customer feedback to inform journey refinement and enable A/B testing. • Clickfox • Medallia • Qualtrics</td>
</tr>
<tr>
<td>Misrepresentation is a type of first party fraud that occurs in both the consumer and commercial businesses. • Income and employment verification • Asset verification • Welcome calls</td>
<td>Correlate data points generated by different systems and channels and employ link analysis to create predictive models on client behaviour. • SAS/R • Splunk • Quantexa • Siren Investigate</td>
<td>Monitor employees for suspicious activity and risk rate abnormal employee behaviour. • BottomLine (Intellinx) • Behavox • Forcepoint • Splunk • Securonix</td>
<td>Enable investigators to manage and examine fraud cases efficiently and effectively. Enforce the use of standardized workflows or ‘playbooks’. • IBM Case Manager • Actimize • BAE</td>
<td>Perform trend analysis, operational performance measurement, and support KPI and KRI reporting. • Tableau • Splunk • Qlikview</td>
<td>Utilize advanced analytics to optimize existing rules and systems to reduce false positives and increase coverage. • SAS • Python • PySpark • R</td>
</tr>
<tr>
<td>First Party Fraud &amp; Misrep</td>
<td>Client Profiling</td>
<td>Internal Fraud Monitoring</td>
<td>Case Management</td>
<td>Reporting</td>
<td>Optimization</td>
</tr>
<tr>
<td>Enforce the use of standardized workflows or ‘playbooks’. • IBM Case Manager • Actimize • BAE</td>
<td>Perform trend analysis, operational performance measurement, and support KPI and KRI reporting. • Tableau • Splunk • Qlikview</td>
<td>Utilize advanced analytics to optimize existing rules and systems to reduce false positives and increase coverage. • SAS • Python • PySpark • R</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
An optimal fraud detection strategy should be supported by a proper technical architecture to identify cross channel, cross product fraud attacks. Companies should invest in big data and advanced analytics to enhance their fraud strategy and client experience.
Big Data and advanced analytics are changing how companies will harness new information sources to make more effective and efficient decisions in fraud prevention.

- **Descriptive Analytics**
  - **What happened?**
  - Diagnostic analytics are useful for understanding an event in hindsight.

- **Diagnostic Analytics**
  - **Why did it happen?**
  - Diagnostic analytics are useful for deriving actionable insights for addressing a specific business issue or historical event.

- **Predictive Analytics**
  - **Why will happen?**
  - Predictive analytics enables analysts to make predictions about future events based upon analysis of recent and historical patterns.

- **Prescriptive Analytics**
  - **What if something else happened?**
  - Prescriptive analytics leverage predictive analytics with actionable data and a feedback system to track the outcomes of business decisions.

**Analytics Maturity Curve**

**Increasing Business Value**

**Increasing Sophistication of Data & Analytics**

**Structured Data and Operational Decisions**

**Unstructured Data and Strategic Decisions**

---

PwC | Institute of internal auditors
Fraud analytics management

An effective fraud analytics solution is a multi-tiered approach that identifies historical trends and patterns, leverages heuristic, calibrated rules and alerts, builds predictive frameworks, uncovers the “unidentified” or “misclassified” true fraud, and continuously evolves over time.

- **Simulation & Capture Of “New” Patterns**
  - Segmentation schemas and simulation of populations into homogeneous groups for investigation; integration of emerging data sources

- **Root Cause & Optimization (Rules/Alerts)**
  - Identify patterns and correlations in confirmed fraud cases
  - Perform root cause analysis and data analysis to identify gaps in the detection

- **Discover the Unknown (Unsupervised)**
  - Unsupervised Learning – Techniques which identify commonalities in behavior without labeled fraud
    - k-Means & k-Modes Clustering
    - Principal Component Analysis
    - Anomaly Detection (various algorithms)
  - Social Network Analysis (Link Analysis)

- **Predictive Modeling (Supervised)**
  - Supervised Learning – Techniques which use historical labeled fraud
    - Regression Analysis
    - Decision Trees/Random Forest
    - Support Vector Machines (SVM)
    - Neural Networks
    - k-Nearest Neighbors
    - Deep Learning
    - Ensemble Techniques

- **Model Development**
  - Simulation & Capture Of “New” Patterns
Unsupervised machine learning is the machine learning task of inferring a function to describe hidden structure from ‘unlabeled’ data (a classification or categorization is not included in the observations). There are several techniques that can be deployed to understand the patterns in data.

### Clustering
This technique aims to segment observations into clusters, each belonging to the cluster with the nearest mean.

The value provided by clustering is to understand the segmentation of observations, providing the ability to identify outlier segments (and their attributes) that may be indicative of risk.

### Social network analysis (Link Analysis)
This technique aims to investigate customer social structures using graph theory to understand relationships of features.

The value provided by social network analysis is to map organizational or customer relationships to uncover hidden relationships that may contribute or detract to related fraud risk.

### Association rules
The technique aims to discover interesting correlations between variables in large datasets.

The value provided by association rules is to quickly uncover how some transactional characteristics may be associated with each other and the ultimate level of potential risk.

### Anomaly detection
This technique identifies observations which do not conform to either an expected pattern or other items in the data set.

The value provided by anomaly detection is the ability to isolate specific outliers in data which have the potential to represent elevated risk due to their non-conformity.
Supervised learning

Supervised learning is the machine learning task of inferring a function from labeled training data. The training data consist of a set of labeled examples. The two most common types of supervised learning are regression (deriving a trend line) and classification (categorizing data points into groups).

**Regression**

This technique models the relationship between variables that is iteratively refined using a measure of error in the predictions made by the model.

The value of regression is the ability to predict an outcome using features and understand the strength of these predictors (features) relative to the outcome.

**Instance-based (Nearest Neighbors)**

This technique classifies observations by referencing the classifications of other observations it is closest to.

The value of this technique is the ability to quickly classify an observation (approximated locally) based on the number of instances “nearest” the observation in question.

**Decision Trees/Random Forests**

This technique identifies features that provide the largest information gain for the purpose of creating homogenous populations of the target class.

The value of decision trees is the versatility of the technique and how easily they can be interpreted when using multiple types of variables. The level of transparency decreases as you begin to ensemble the trees (Random Forest).

**Deep learning via neural networks**

This technique trains layers of “neurons” that are activated by input data; activations are propagated to subsequent layers, reaching a final layer for prediction.

The value of using this technique is primarily found when solving extremely complex and abstract problems, such as image or voice recognition.
Agile approach

We recommend leveraging an iterative, parallel approach to assessing and augmenting an organization’s fraud analytics program. Similar approaches can be leverage in order to conduct risk-based testing of fraud controls and their effectiveness.

Assess & Standardize
- Review and understand existing relevant data sets (customer, account, financial & non-financial transactions, authentication, etc.) and their mapping to anomaly detection rules
- Analyze existing rule sets based on detection coverage, alert volumes, sensitivity (true positive) and specificity (true negative), and type I and II error
- Standardize all decision science within current inventory of anomaly detection rules
- Identify opportunities to leverage additional data and anomaly detection rules

Augment & Optimize
- Review design of data structure to include relevant dispersed data sets
- Conduct unsupervised and/or supervised learning techniques to evaluate discriminatory features for fraud detection
- Suggest new anomaly detection rules leveraging unified data set and engineered features
- Optimize the final anomaly detection rule set based on fraud loss objective function(s); including potential back testing and simulation

Automate, Prioritize & Promote
- Develop microservices in agile sprints to automate data processing, anomaly detection decision science, fusion and prioritization, and promotion to visualization and case management
- Identify relevant performance monitoring including KPIs and alerting processes to support ongoing optimization
- Develop implementation plan for future rules/models optimization including champion and challenger development environments and gradual deployment to production environment
Reflection question 5

Which of the following analytical techniques is most preferred within your Internal Audit function in connection with an assessment and testing of anti-fraud controls in your organization?

A. Random sampling of transactions, and/or fraud alerts/cases across business units, products, etc., for manual testing against documented procedures

B. Judgmental sampling of items that appear to be extreme outliers relative to the general population, but performed using a manual or semi-manual approach (sorting, browsing, etc.)

C. Algorithmic based selection of anomalous or suspect items, leveraging anomaly detection techniques, statistical outlier analysis, Benford's Law analytics, etc.

D. None of the above/something else
Reflection question 6

How often do you conduct a fraud-focused internal audit at your organization?

A. Every Year
B. Every Other Year
C. Once every 3 years
D. Once every 4 years
E. None of the Above
Reflection question 7

In which of the following areas is Internal Audit most involved in your organization (hours delivered)?

A. Participating in the Fraud Risk Assessment process
B. Performing special investigations related to fraud incidents
C. Performing defect analysis, root cause analysis, post mortem reviews of significant fraud events
D. Performing operating effectiveness testing of anti-fraud controls
E. Performing fraud awareness training
Thank you