Deloitte.

Data analytics for Fraud Waste and Abuse

Practical benefits and considerations

National Association for Medicaid Program Integrity

Sriram Krishnan, PhD
Mike Little

Deloitte Financial Advisory Services LLP

August 2013

Fraud, waste, and abuse examples

- Billing for services not rendered
- Double billing
- Substitution of generic drugs
- Diversion of drugs
- Unnecessary services
- Kickbacks
- Cost report manipulation
- Unbundling
- Identity theft/use of provider numbers

Traditional models

- Hotlines
- EOMBs
- Complaints/whistleblowers
- Informants
- Investigative leads
- Post payment review
- Post payment audit
- Prepayment review
- Edits
- Data mining

We go out and investigate and we get results…

Investigative results

- In the five and a half years since its inception, Strike Force prosecutors filed more than 724 cases charging more than 1,476 defendants who collectively billed the Medicare program more than $4.6 billion; 918 defendants pleaded guilty and 105 others were convicted in jury trials; and 745 defendants were sentenced to imprisonment for an average term of more than 45 months.

  Source: DOJ and HHS HCFAC report for 2012

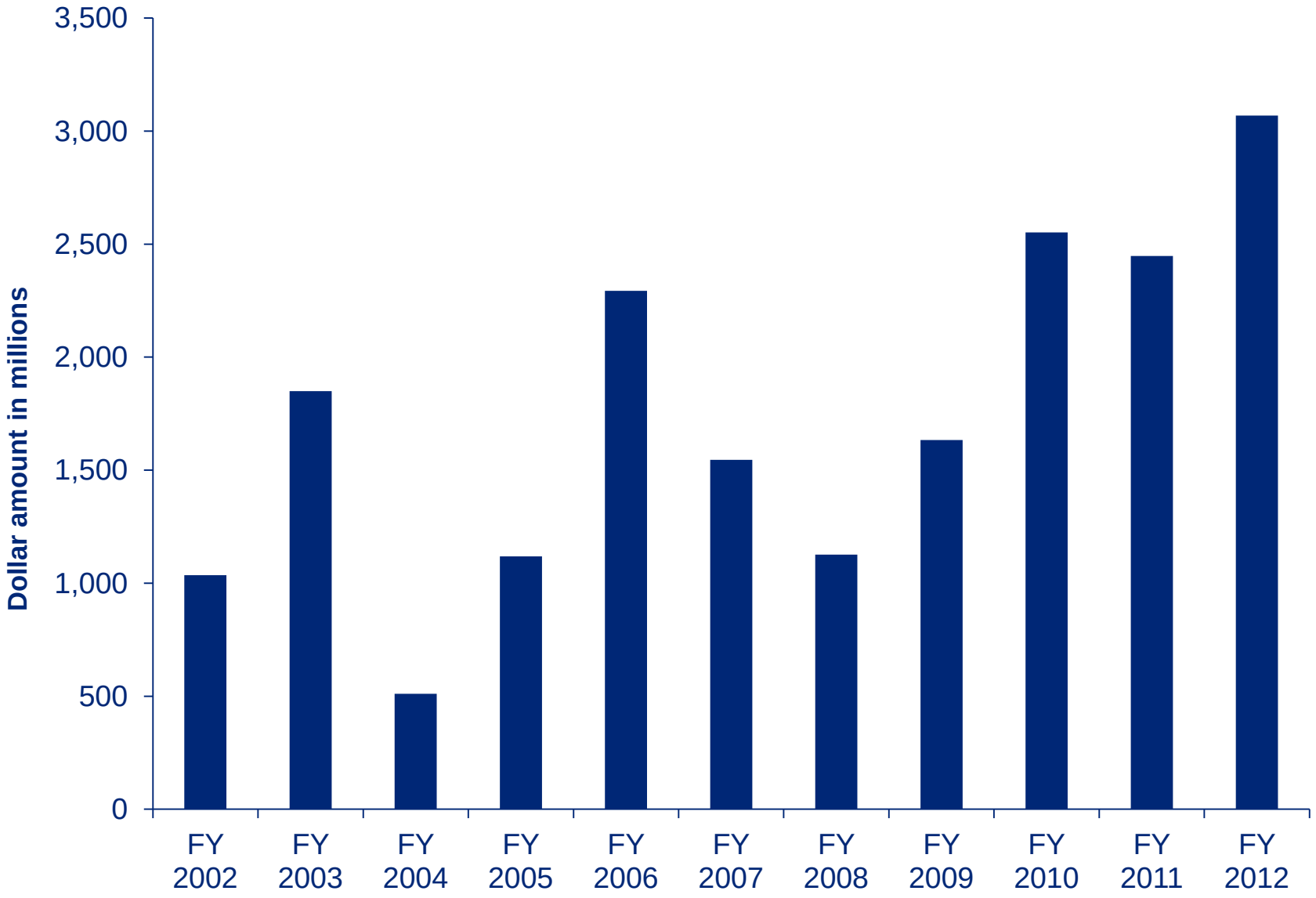
- Collectively in FY 2012, the MFCUs reported conducting 15,531 investigations, Investigations resulted in 1,359 individuals being indicted or criminally charged: 995 for fraud and 364 for patient abuse and neglect. In total, 1,337 convictions were reported in FY 2012, of which 982 were related to Medicaid fraud and 355 were related to patient abuse and neglect. The total number of civil judgments and settlements for the fiscal year was 823. In FY 2012, States reported $2.9 billion in recoveries for both civil and criminal cases handled by the 50 MFCUs. In addition to other significant accomplishments by the MFCUs in prosecuting patient abuse and detecting and deterring fraud, this translates to a return on investment (ROI) of $13.48 per $1 expended by the Federal and State Governments for MFCU operations.

  Source: HHS/OIG report on MFCUs

- The return-on-investment (ROI) for the HCFAC program over the last three years (2010–2012) is $7.90 returned for every $1.00 expended.

  Source: DOJ and HHS HCFAC report for 2012

FCA health care recoveries



Source: As reported by the Department of Justice, 2013

FWA in Medicare/Medicaid

- Combined federal and state spending on Medicaid and Medicare is projected to exceed $800 billion per year in 2010. While there is no **official federal estimate of the level of fraud** in Medicare, Medicaid or the healthcare sector more generally, external estimates project the amount at **three to ten percent** of total spending, that could correlate to **$27 to $80 billion in 2010** alone, if left unchecked…

Source: Acting Deputy Attorney General Gary G. Grindler remarks at the National Institute on Health Care Fraud Miami Thursday, May 13, 2010

FWA in Medicare/Medicaid

- Chairman Joe Pitts (R-PA) pointed out in his opening statement that 21 percent of Medicare payments and 15 percent of Medicaid total expenditures are inappropriate payments. Pitts stated that, “In an April 2012 study, former CMS Administrator Donald M. Berwick and RAND Corporation analyst Andrew D. Hackbarth estimated that fraud and abuse added as much as $98 billion to Medicare and Medicaid spending in 2011.”

  Source: House Energy and Commerce Health Subcommittee hearing entitled “Fostering Innovation to Fight Waste, Fraud and Abuse in Health Care.”

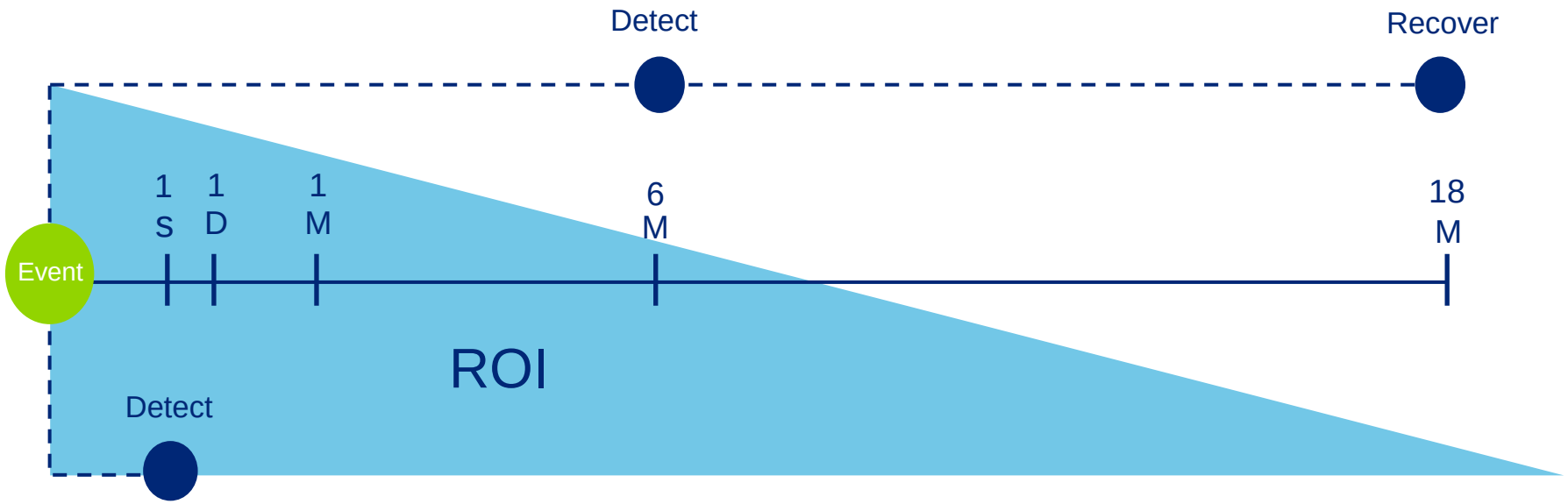
  A study from the Institute of Medicine estimated health care fraud at $75 billion a year and found that about 30 percent of total U.S. health spending in 2009 — roughly $750 billion — was wasted on unnecessary services, excessive administrative costs, fraud and other problems.

  Source: New York Times, published September 11, 2012

“PAY and CHASE” is DEAD

DETECT and PREVENT is the future

Paradigm shift: From “Pay-and-Chase” to “Prevention”

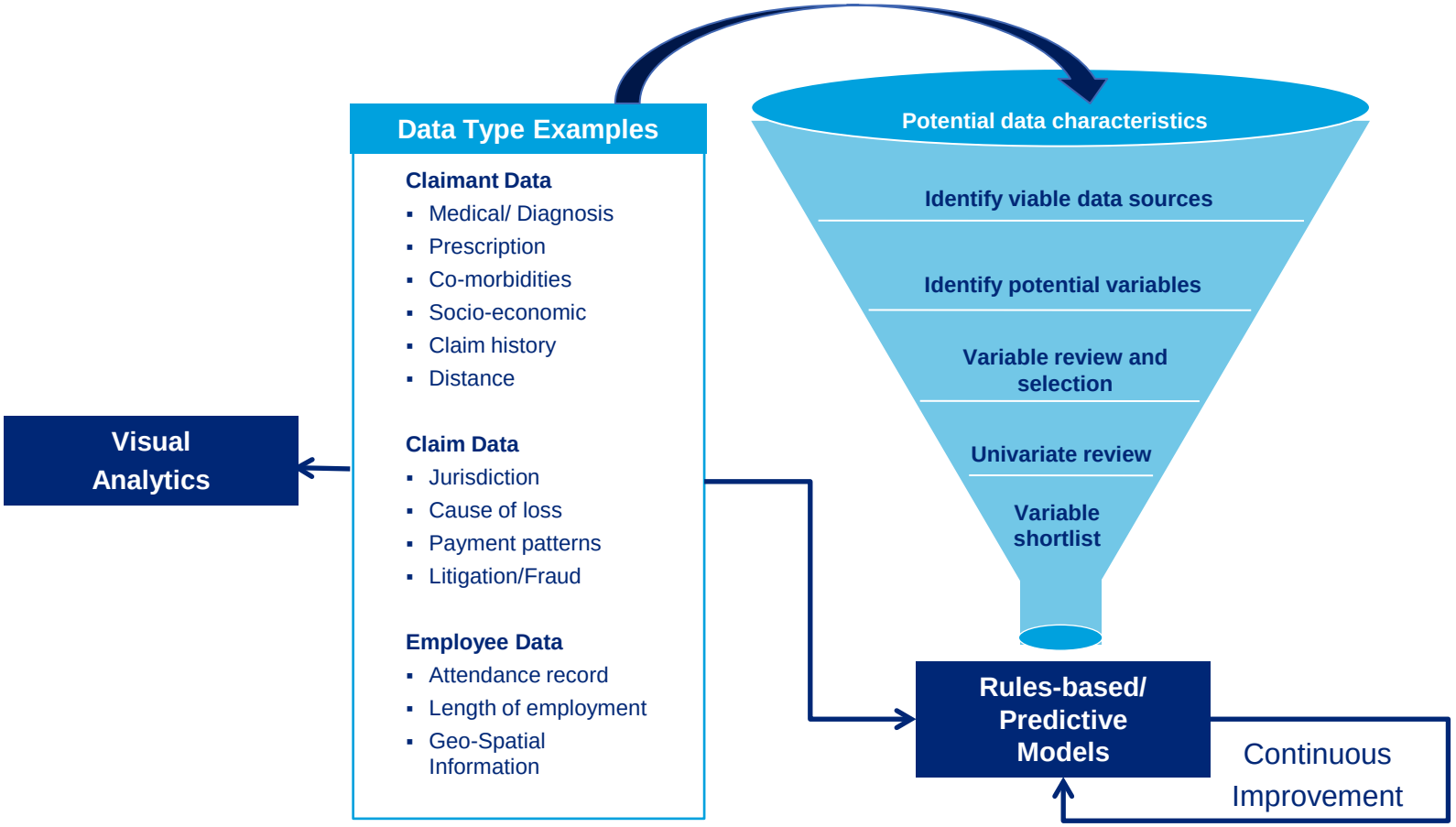


Goals for this section

- What is analytics?
  - What considerations should we make when applying analytics to fraud/waste/abuse?
- How to think about analytics within the overall workflow of program integrity?
- How should I go about thinking about implementing analytics to address fraud/waste/abuse?

What is analytics?

A variety of tools and methods to visualize, summarize, extrapolate and otherwise use data to get insights into fraudulent behavior, with the goal of preventing, detecting and monitoring fraud.

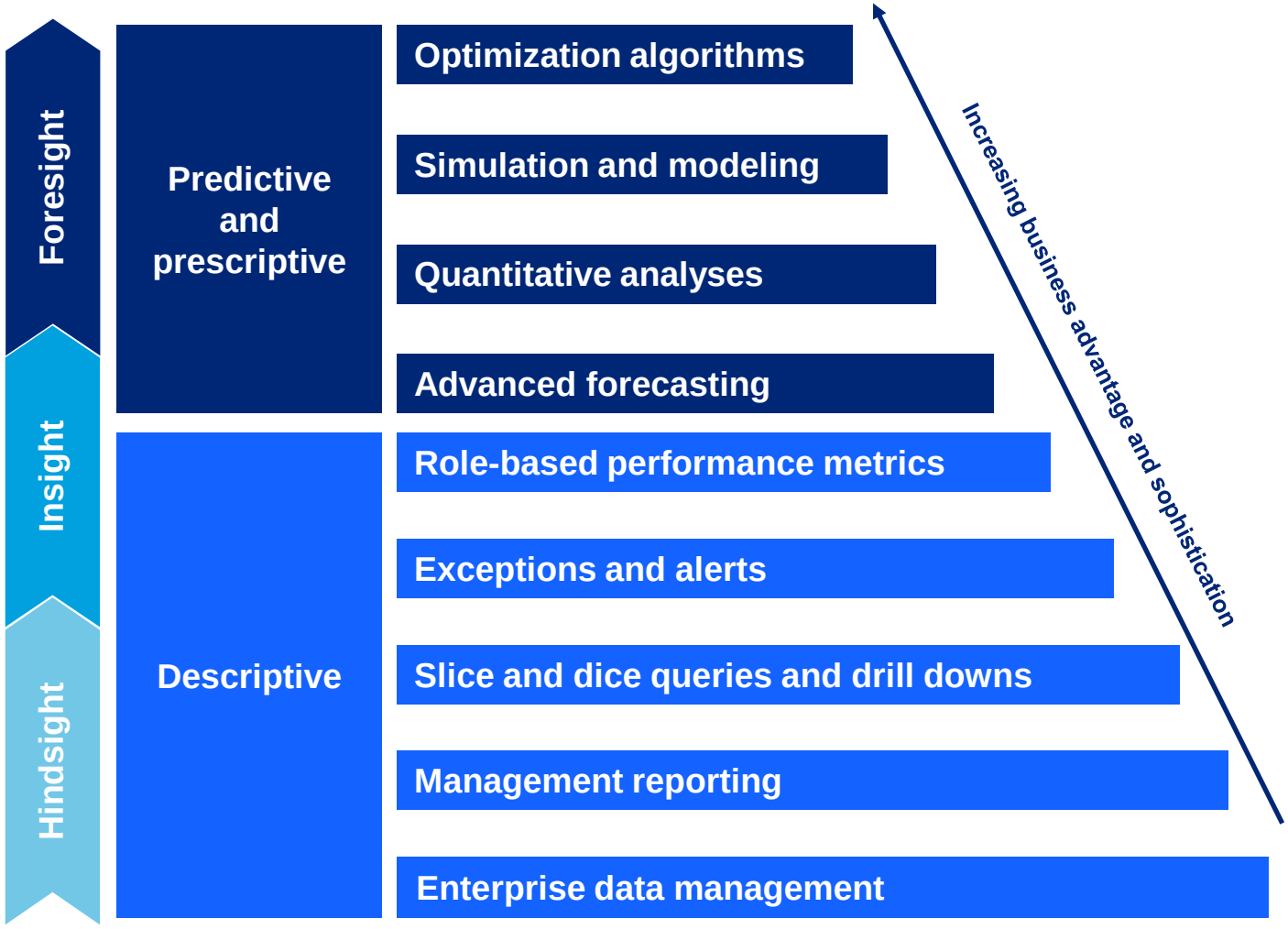


Apply analytics to provide hindsight, insight, and foresight by leveraging data

Understand the signals generated across your ecosystem to shape the future

Use data from within the organization to drive changes here and now

Conduct “rear-view mirror” assessments based on data generated by operations

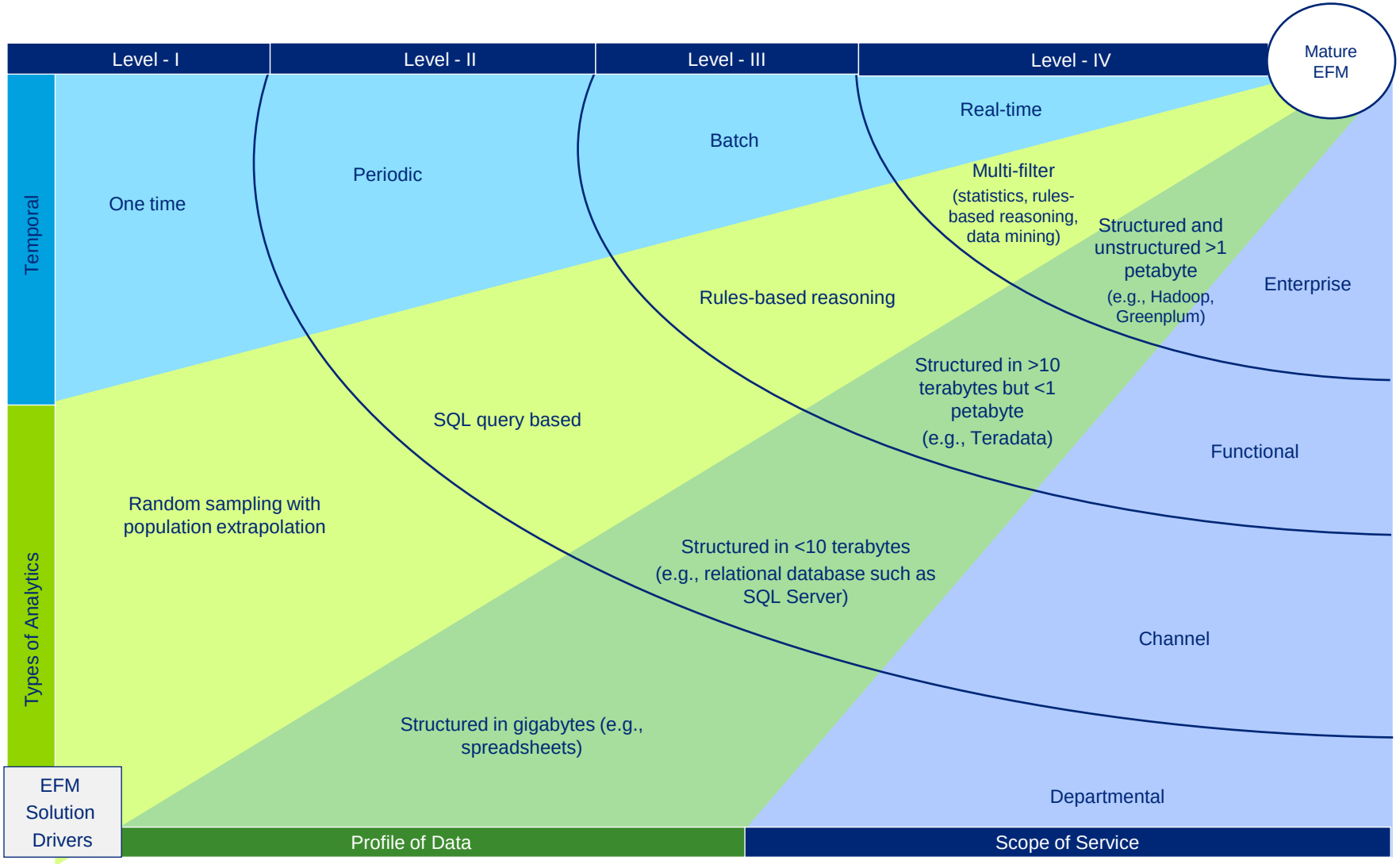


Leverage lessons learned from other industries

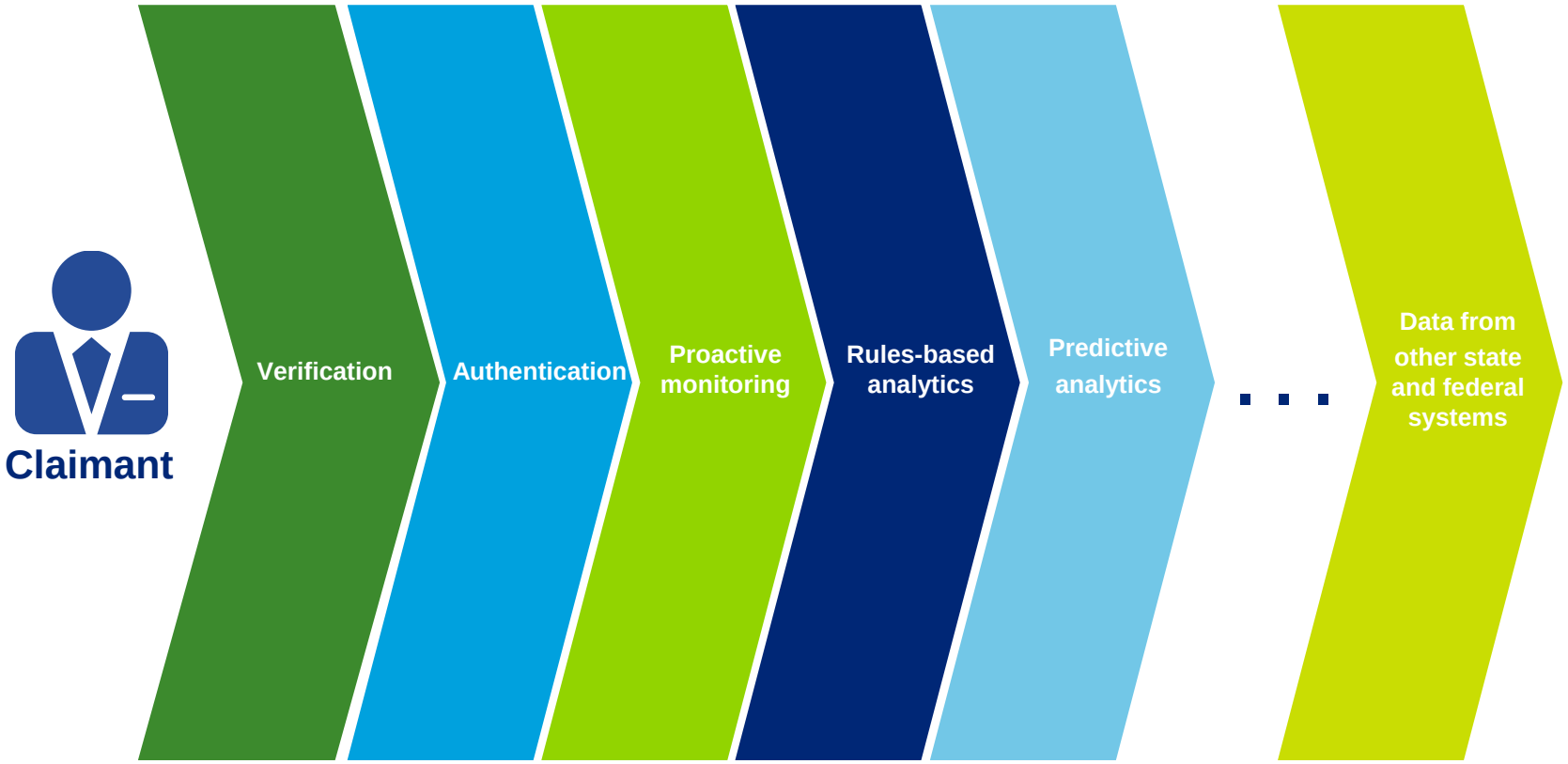
- Other industries have a long history of fraud detection, and have developed mature models and solutions
  - Credit card — detection of potentially fraudulent purchases
  - Anti-money laundering — monitoring financial transactions
  - Telecommunications — detect handset fraud and financial fraud

13

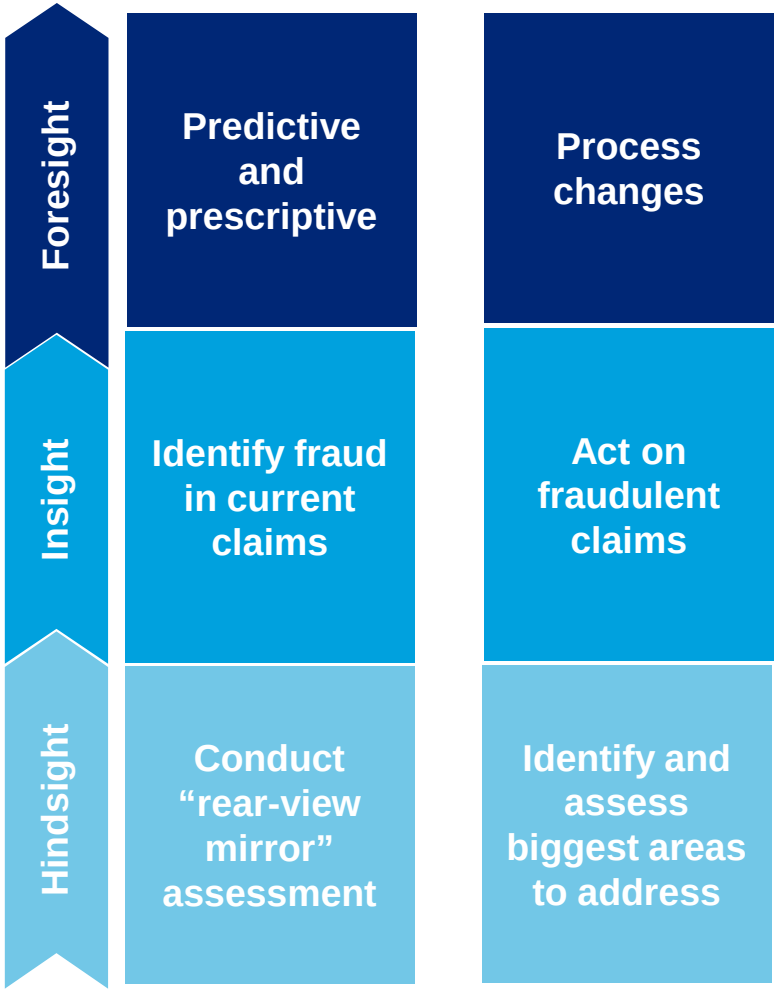
Solution drivers for Enterprise Fraud Management (EFM)



What kind of fraud detection?
Multiple layers of anti-fraud defense



Three steps to applying analytics



Step 1: Hindsight

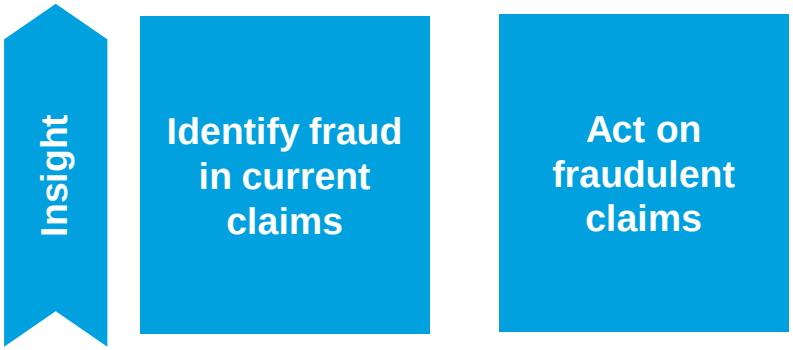
Identify high-risk areas, and what should be done

Identify biggest areas to address with fraud

- What are considerations of your state
  - FFS vs. managed care
  - Do you believe that Medicaid expansion is an area of concern
- Begin with a one-time assessment: where are biggest potential areas of fraud?
  - Take a set of claims data, and apply against a set of rules
  - Use this to identify potential areas of improvement, and where to target
  - Combine with heuristic approach looking at areas of weakness — what will bring the biggest bang for the buck?

Step 2: Insight

Apply analytics to find fraud



- Data from Hindsight step is used to prioritize aspects of FWA to address
- Analytics approach
  - Apply models against claims data to identify potential FWA
  - Can be done post-adjudication (in batch mode) or pre-adjudication (as claims come in)
- This step requires process change management, and understanding of how to act on potential FWA issues

Critical capabilities for EFM vendors

Product vendors and service providers should provide a range of integrated capabilities to be competitive in the crowded EFM marketplace.

Capability	Functionality overview
Real-time transaction support	Detection of fraud near the point of transactional origination before it can be ultimately fulfilled
Entity link analysis	Analysis of relationships in both internal and entities to prevent collusive or organized criminal behavior
“Canned” intelligence and analytics	Availability of rules or predictive models integrated into the platform that can be run “out of the box”
Business user interface for alert and policy management	Support the creation, management, investigation, and workflow of fraud alerts
Deployment and support simplicity	Ability to integrate with complex and disparate legacy financial and accounting systems
Channel- and product-specific coverage	Ability to apply and tailor the solution across channels and business product lines

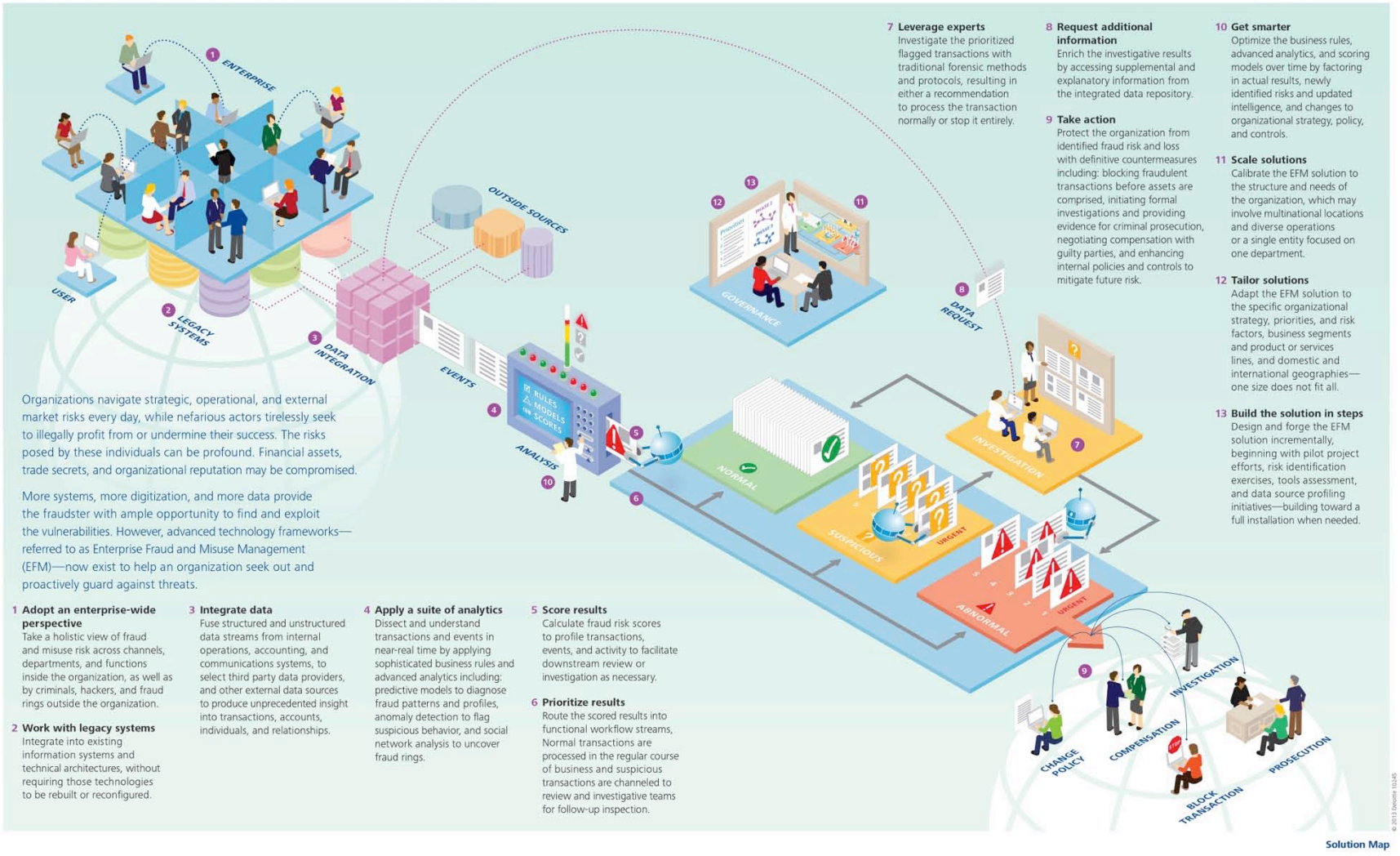
Source: Gartner Analyst Report

Step 3: Foresight

Continuous improvement

- Data from Insight step is used to improve process and workflow, and identify changing areas of FWA
- Analytics approach
  - Use of pattern recognition to identify and monitor anomalies
  - Combining data from other state and federal systems to identify complex fraud
- Use results of analytics to suggest process changes and further improvements

Bring analytics within workflow



Organizations navigate strategic, operational, and external market risks every day, while nefarious actors tirelessly seek to illegally profit from or undermine their success. The risks posed by these individuals can be profound. Financial assets, trade secrets, and organizational reputation may be compromised.

More systems, more digitization, and more data provide the fraudster with ample opportunity to find and exploit the vulnerabilities. However, advanced technology frameworks—referred to as Enterprise Fraud and Misuse Management (EFM)—now exist to help an organization seek out and proactively guard against threats.

1 Adopt an enterprise-wide perspective
Take a holistic view of fraud and misuse risk across channels, departments, and functions inside the organization, as well as by criminals, hackers, and fraud rings outside the organization.

2 Work with legacy systems
Integrate into existing information systems and technical architectures, without requiring those technologies to be rebuilt or reconfigured.

3 Integrate data
Fuse structured and unstructured data streams from internal operations, accounting, and communications systems, to select third party data providers, and other external data sources to produce unprecedented insight into transactions, accounts, individuals, and relationships.

4 Apply a suite of analytics
Dissect and understand transactions and events in near-real time by applying sophisticated business rules and advanced analytics including: predictive models to diagnose fraud patterns and profiles, anomaly detection to flag suspicious behavior, and social network analysis to uncover fraud rings.

5 Score results
Calculate fraud risk scores to profile transactions, events, and activity to facilitate downstream review or investigation as necessary.

6 Prioritize results
Route the scored results into functional workflow streams. Normal transactions are processed in the regular course of business and suspicious transactions are channeled to review and investigative teams for follow-up inspection.

7 Leverage experts
Investigate the prioritized flagged transactions with traditional forensic methods and protocols, resulting in either a recommendation to process the transaction normally or stop it entirely.

8 Request additional information
Enrich the investigative results by accessing supplemental and explanatory information from the integrated data repository.

9 Take action
Protect the organization from identified fraud risk and loss with definitive countermeasures including: blocking fraudulent transactions before assets are comprised, initiating formal investigations and providing evidence for criminal prosecution, negotiating compensation with guilty parties, and enhancing internal policies and controls to mitigate future risk.

10 Get smarter
Optimize the business rules, advanced analytics, and scoring models over time by factoring in actual results, newly identified risks and updated intelligence, and changes to organizational strategy, policy, and controls.

11 Scale solutions
Calibrate the EFM solution to the structure and needs of the organization, which may involve multinational locations and diverse operations or a single entity focused on one department.

12 Tailor solutions
Adapt the EFM solution to the specific organizational strategy, priorities, and risk factors, business segments and product or services lines, and domestic and international geographies—one size does not fit all.

13 Build the solution in steps
Design and forge the EFM solution incrementally, beginning with pilot project efforts, risk identification exercises, tools assessment, and data source profiling initiatives—building toward a full installation when needed.

Solution Map

Recommendations on how to leverage analytics

1. Understand the issues to be addressed
   - What will our Medicaid program look like going forward?
   - What are the biggest issues that are faced in our state regarding fraud/waste/abuse?
   - Strongly consider a one-time analytics assessment

2. Understand the whole process
   - Look at whole process — how would we modify our workflow to incorporate analytics?
   - Who are primary stakeholders, and how will we get buy-in?
   - Implement change process

This presentation contains general information only and Deloitte Financial Advisory Services LLP is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte Financial Advisory Services LLP shall not be responsible for any loss sustained by any person who relies on this presentation.

Deloitte.

Official Professional Services Sponsor

Professional Services means audit, tax, consulting and financial advisory services.