



Contacts

Brien Lorenze
Principal
Deloitte Advisory
Email: blorenze@deloitte.com
Tel: +1 571 814 7560

Dan Olson, CFE
Senior Manager
Deloitte Advisory
Deloitte Transactions and Business Analytics LLP
Email: danolson@deloitte.com
Tel: +1 312 965 3617



As used in this document, "Deloitte Advisory" means Deloitte & Touche LLP, which provides audit and enterprise risk services; Deloitte Financial Advisory Services LLP, which provides forensic, dispute, and other consulting services; and its affiliate, Deloitte Transactions and Business Analytics LLP, which provides a wide range of advisory and analytics services. Deloitte Transactions and Business Analytics LLP is not a certified public accounting firm. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication 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, its affiliates, and related entities shall not be responsible for any loss sustained by any person who relies on this publication.

Copyright © 2017 Deloitte Development LLC. All rights reserved.

Health Care Program Integrity

Proactively protecting government and commercial entities from the threat of fraud, waste, and abuse

Solution map

Health care fraud, waste, and abuse

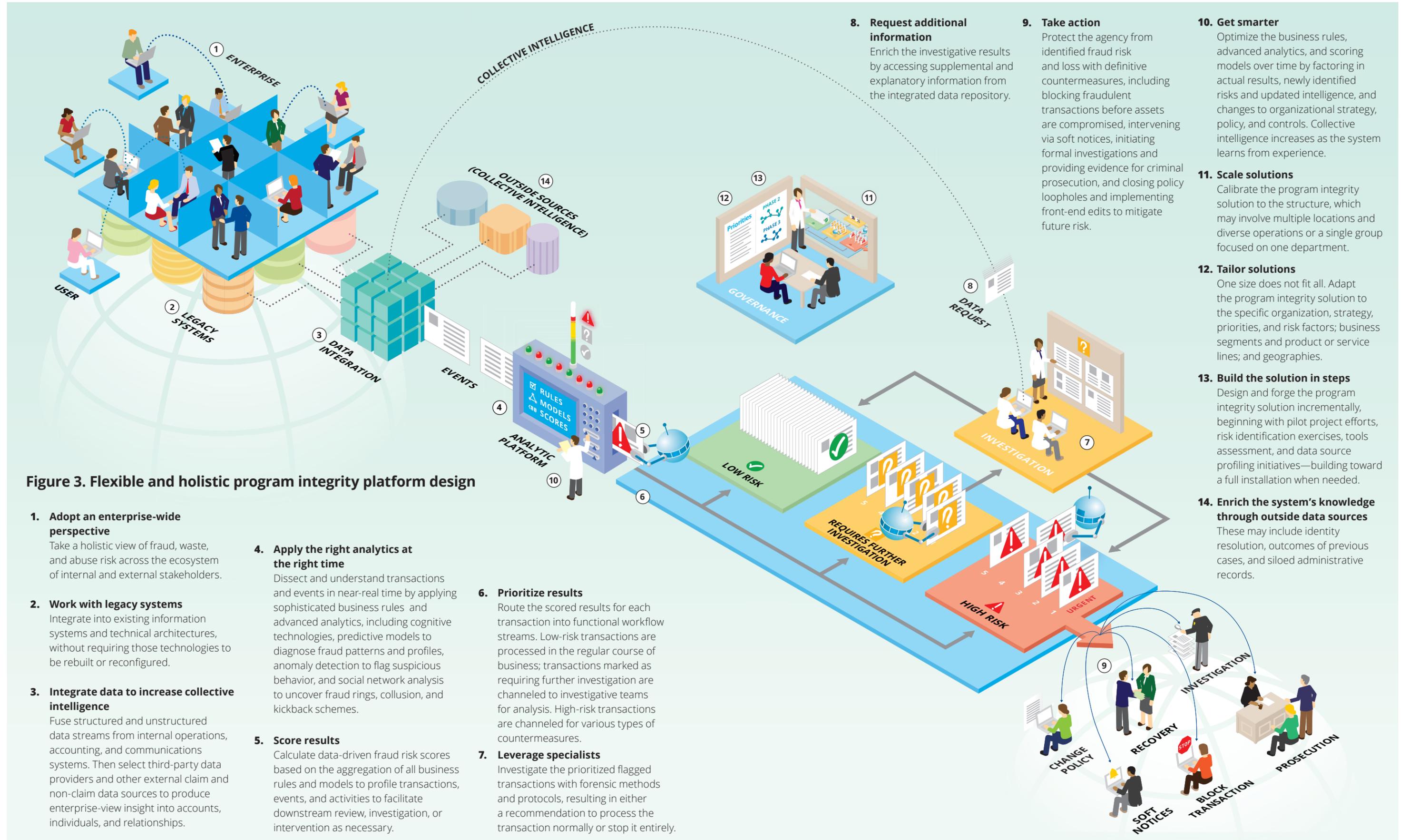


Figure 3. Flexible and holistic program integrity platform design

1. Adopt an enterprise-wide perspective

Take a holistic view of fraud, waste, and abuse risk across the ecosystem of internal and external stakeholders.

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 to increase collective intelligence

Fuse structured and unstructured data streams from internal operations, accounting, and communications systems. Then select third-party data providers and other external claim and non-claim data sources to produce enterprise-view insight into accounts, individuals, and relationships.

4. Apply the right analytics at the right time

Dissect and understand transactions and events in near-real time by applying sophisticated business rules and advanced analytics, including cognitive technologies, predictive models to diagnose fraud patterns and profiles, anomaly detection to flag suspicious behavior, and social network analysis to uncover fraud rings, collusion, and kickback schemes.

5. Score results

Calculate data-driven fraud risk scores based on the aggregation of all business rules and models to profile transactions, events, and activities to facilitate downstream review, investigation, or intervention as necessary.

6. Prioritize results

Route the scored results for each transaction into functional workflow streams. Low-risk transactions are processed in the regular course of business; transactions marked as requiring further investigation are channeled to investigative teams for analysis. High-risk transactions are channeled for various types of countermeasures.

7. Leverage specialists

Investigate the prioritized flagged transactions with 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 agency from identified fraud risk and loss with definitive countermeasures, including blocking fraudulent transactions before assets are compromised, intervening via soft notices, initiating formal investigations and providing evidence for criminal prosecution, and closing policy loopholes and implementing front-end edits 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. Collective intelligence increases as the system learns from experience.

11. Scale solutions

Calibrate the program integrity solution to the structure, which may involve multiple locations and diverse operations or a single group focused on one department.

12. Tailor solutions

One size does not fit all. Adapt the program integrity solution to the specific organization, strategy, priorities, and risk factors; business segments and product or service lines; and geographies.

13. Build the solution in steps

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

14. Enrich the system's knowledge through outside data sources

These may include identity resolution, outcomes of previous cases, and siloed administrative records.