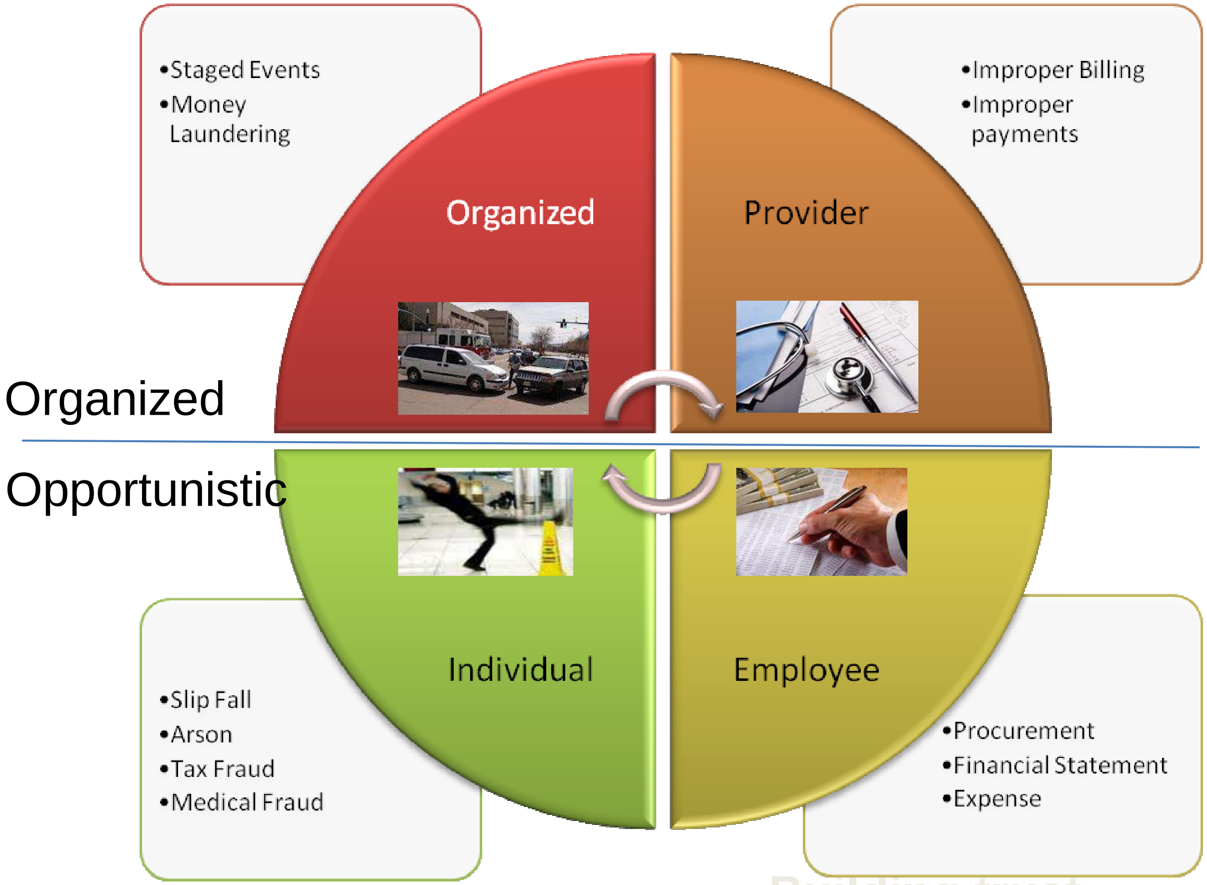
IBM
FRAUD ÇÖZÜMLERİ

13 Mart 2014

Fraud, a deliberate misrepresentation which violates a legal statute and is intended to produce an undue financial gain



Organized

- Staged Events
- Money Laundering

Provider

- Improper Billing
- Improper payments

Opportunistic

Individual

- Slip Fall
- Arson
- Tax Fraud
- Medical Fraud

Employee

- Procurement
- Financial Statement
- Expense

Related areas

Abuse – the same as a Fraud, but not determined to be illegal

Threat - similar to Fraud but for non-financial gain (i.e. political, etc.)

Financial Crime - includes AML, cyber attack, or illegal security breach

Fraud’s economic impact and key trends

> “U.S. organizations lose an estimated 7 percent of annual revenues to fraud… this percentage indicates a staggering estimate of losses around **$994 billion** among organizations, despite increased emphasis on anti-fraud controls and recent legislation to combat fraud.”

Trends

- Crime rings are increasingly turning to fraud
- Economic downturns lead to greater fraud and abuse
- Market conditions pressuring bottom lines
- Complexity and sophistication of fraud schemes are rapidly increasing
- Interest in finding and fighting fraud is rising in priority for public and private organizations
- Advances in analytics are enabling finding and preventing fraud both possible & economical

REPORT TO THE NATIONS
ON OCCUPATIONAL FRAUD AND ABUSE

2012 GLOBAL FRAUD STUDY

ACFE

Reference: 2012 “Report to the Nations”
Association of Certified Fraud Examiners

Evolving challenges and response

•Financial impact

•7% of revenue (ACFE)

•$3.5tn per annum (ACFE)

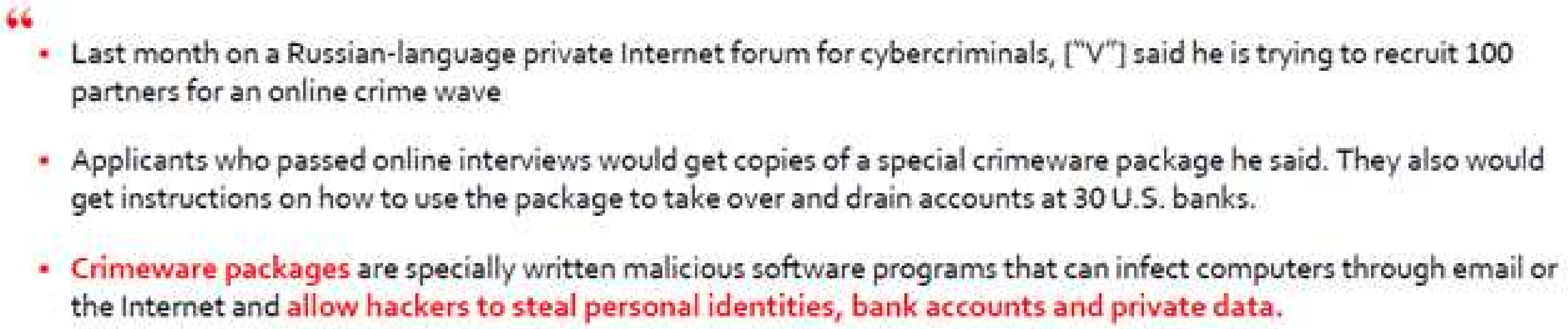
Regulator fines

HSBC $1.9B

ING $619M….

Brand/reputation

Damage to shareholder value (much greater than fine)



“

- Last month on a Russian-language private Internet forum for cybercriminals, ["V"] said he is trying to recruit 100 partners for an online crime wave
- Applicants who passed online interviews would get copies of a special crimeware package he said. They also would get instructions on how to use the package to take over and drain accounts at 30 U.S. banks.
- Crimeware packages are specially written malicious software programs that can infect computers through email or the Internet and allow hackers to steal personal identities, bank accounts and private data.

Nearly half of directors (46%) say their boards have held additional discussions about the “tone at the top” of the company as part of their focus on mitigating fraud risks.

www.pwc.com

…12% of companies reported an overall increase in fraud

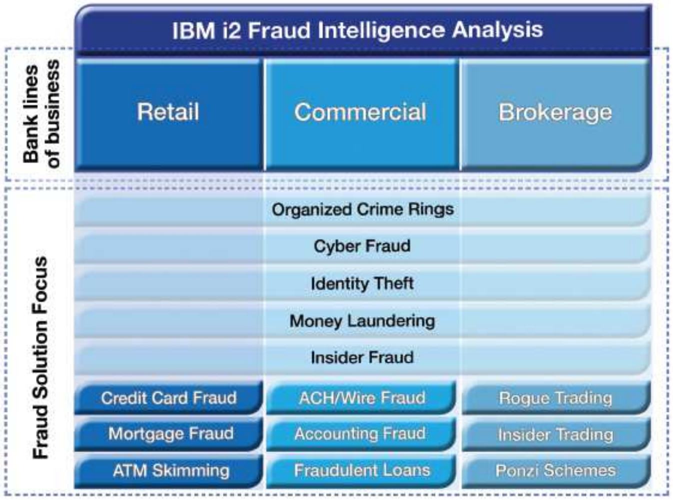
(IBM CIO risk study)

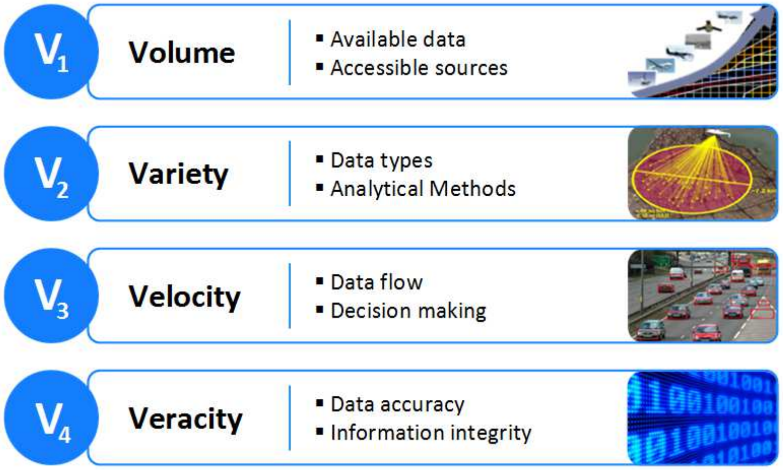
“Fraud is difficult to measure … which means some of the fraud loss figures … only reflect fraud that has been reported. As a result, the fraud figure underestimates the total financial loss resulting from fraud.”

— National Fraud Authority: Annual fraud indicator. January 2010.

Challenges faced by Financial Services

- Regular and complex attacks
- Threat to brand and reputation
- Ever tightening regulatory environment
- Boardroom agenda “tone at the top”
- Complex multi-channel (online, mobile, call center, cross-brand etc) customer interaction and processes……..





…and this data hides “intelligence”

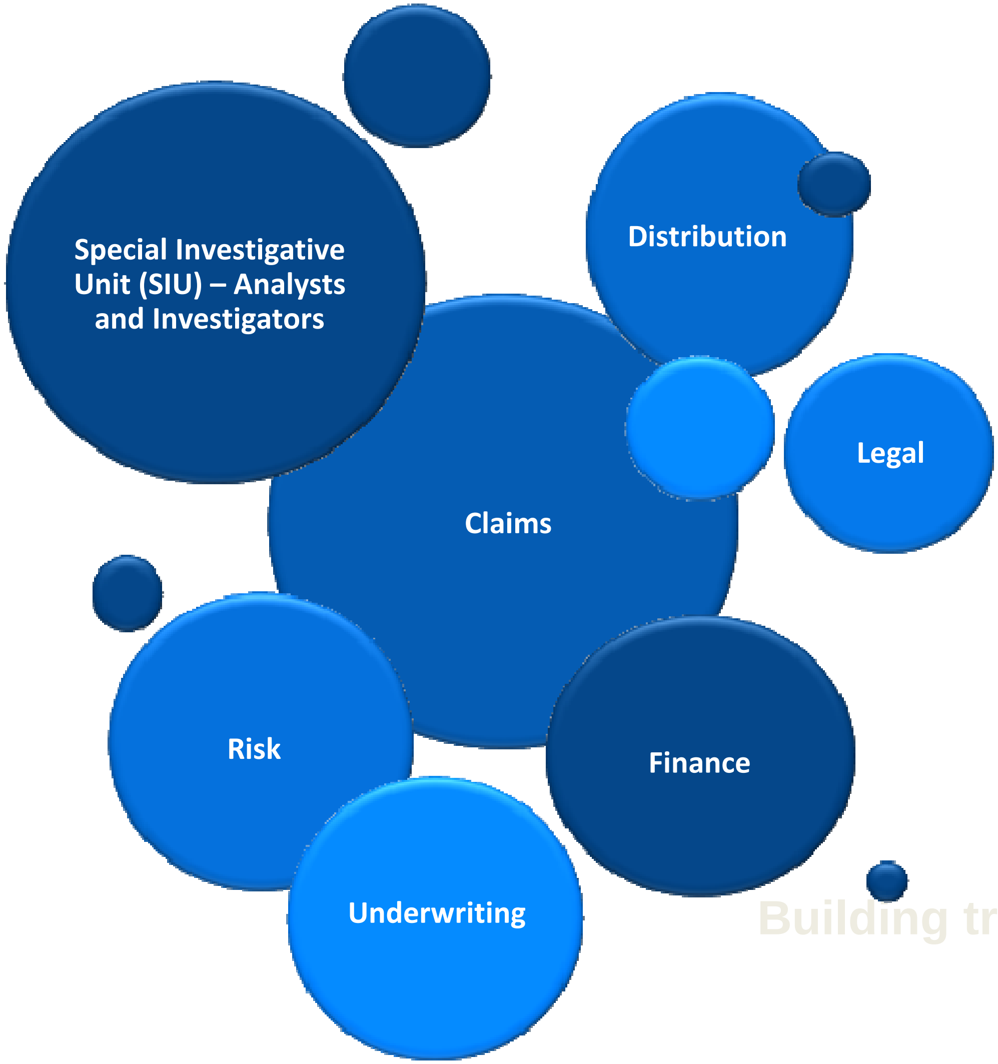
Data growth - 90% of worlds data created in the last two years

Criminals take advantage of complexity

Investigation is only possible by joining all relevant information

- **and must be completed quickly to minimize the costs and impact**

The primary challenge for companies today is the “observation” space is silo’s – making it hard to find fraudsters



Special Investigative Unit (SIU) – Analysts and Investigators

Distribution

Claims

Legal

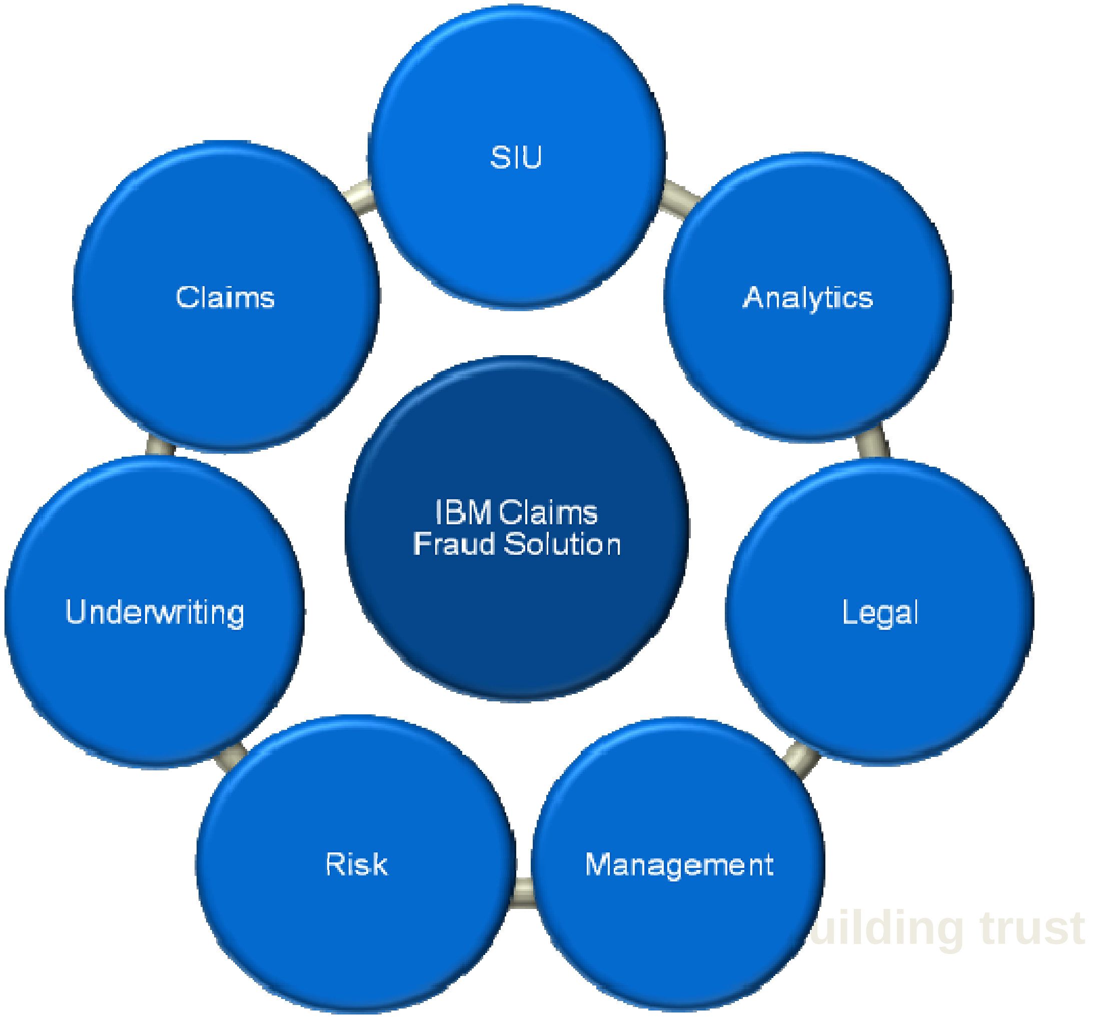
Risk

Finance

Underwriting

- Business units that use point solutions are more likely to miss fraudulent activity
- Silo’d systems create gaps between intelligence units
- Disconnected and niche fraud solutions drive up I.T. costs and resources
- Transparency and compliance reporting is difficult to support
- Taking action against fraudulent intelligence is prolonged

Advances in Big Data and Analytics allow us to expand the observation space by aggregating the data across the enterprise



- Reduces complexity across lines of business
- Allows management of fraud pervasively across the enterprise
- Improves transparency with fraud intelligence sharing
- Increases productivity and created actionable intelligence to predict, detect, discover, and manage fraud

Integrate investigation silos to optimize response and value

Fraud

- Investigate and document fraud and financial crime to disrupt fraud or support case for prosecution

Cyber

- Analyze and visualize cyber threats and impact to understand breadth and impact

Anti-Money Laundering

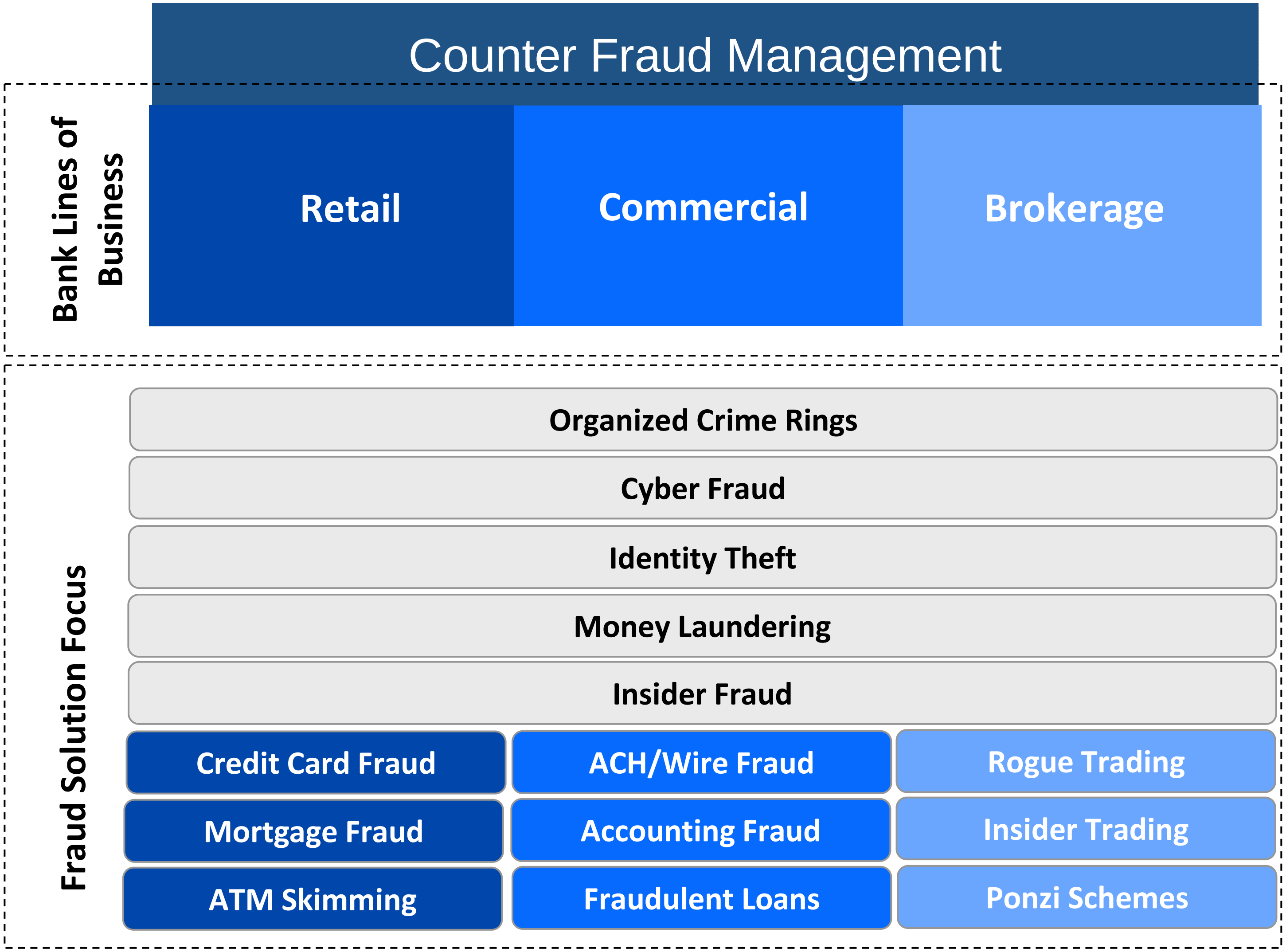
- Investigate (EDD) and document transactions to improve Compliance and

Connecting (traditionally) siloed domains significantly improves defense against emerging attacks

Building trust

’banking institutions should be concerned about fraud attempts linked to recent distributed-denial-of-service attacks on prominent banks.’

Fraud and money laundering use case examples



Counter Fraud Management

Bank Lines of Business

Retail

Commercial

Brokerage

Fraud Solution Focus

Organized Crime Rings

Cyber Fraud

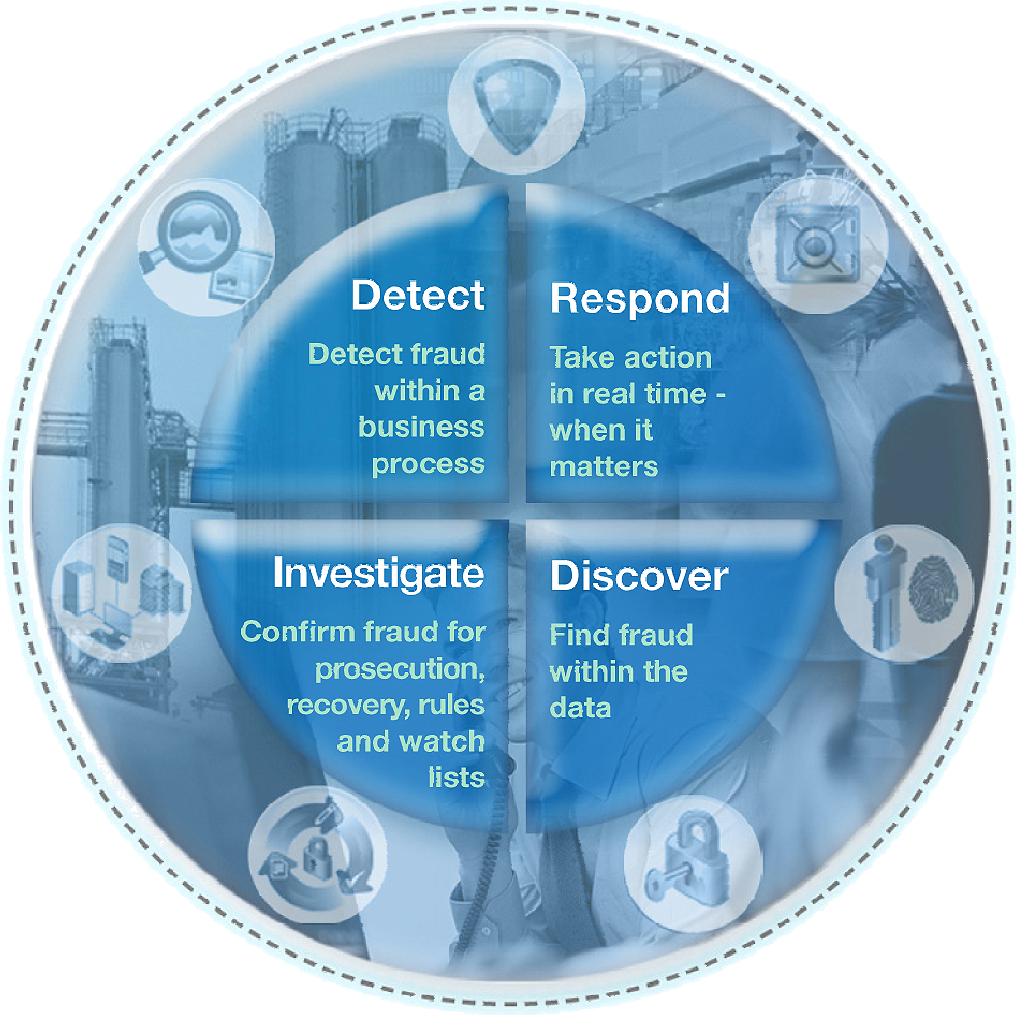
Identity Theft

Money Laundering

Insider Fraud

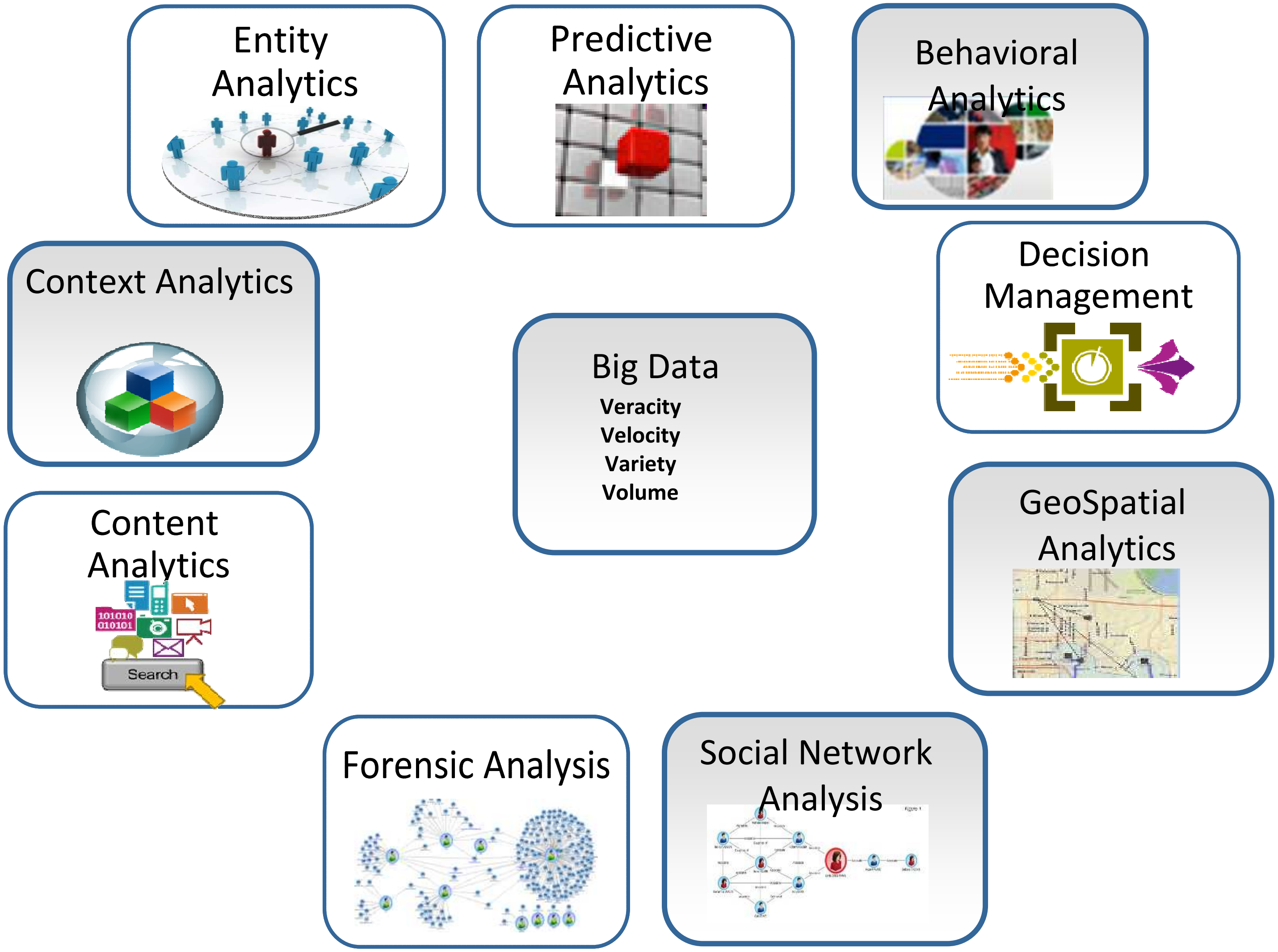
Retail	Commercial	Brokerage
Credit Card Fraud	ACH/Wire Fraud	Rogue Trading
Mortgage Fraud	Accounting Fraud	Insider Trading
ATM Skimming	Fraudulent Loans	Ponzi Schemes

Counter-Fraud Management addresses each phase of an enterprise fraud approach



Detect
Detect fraud within a business process
Respond
Take action in real time - when it matters
Investigate
Confirm fraud for prosecution, recovery, rules and watch lists
Discover
Find fraud within the data

Counter-Fraud Management addresses each phase of an enterprise fraud approach



Entity Analytics

Predictive Analytics

Behavioral Analytics

Context Analytics

Big Data

Veracity
Velocity
Variety
Volume

Decision Management

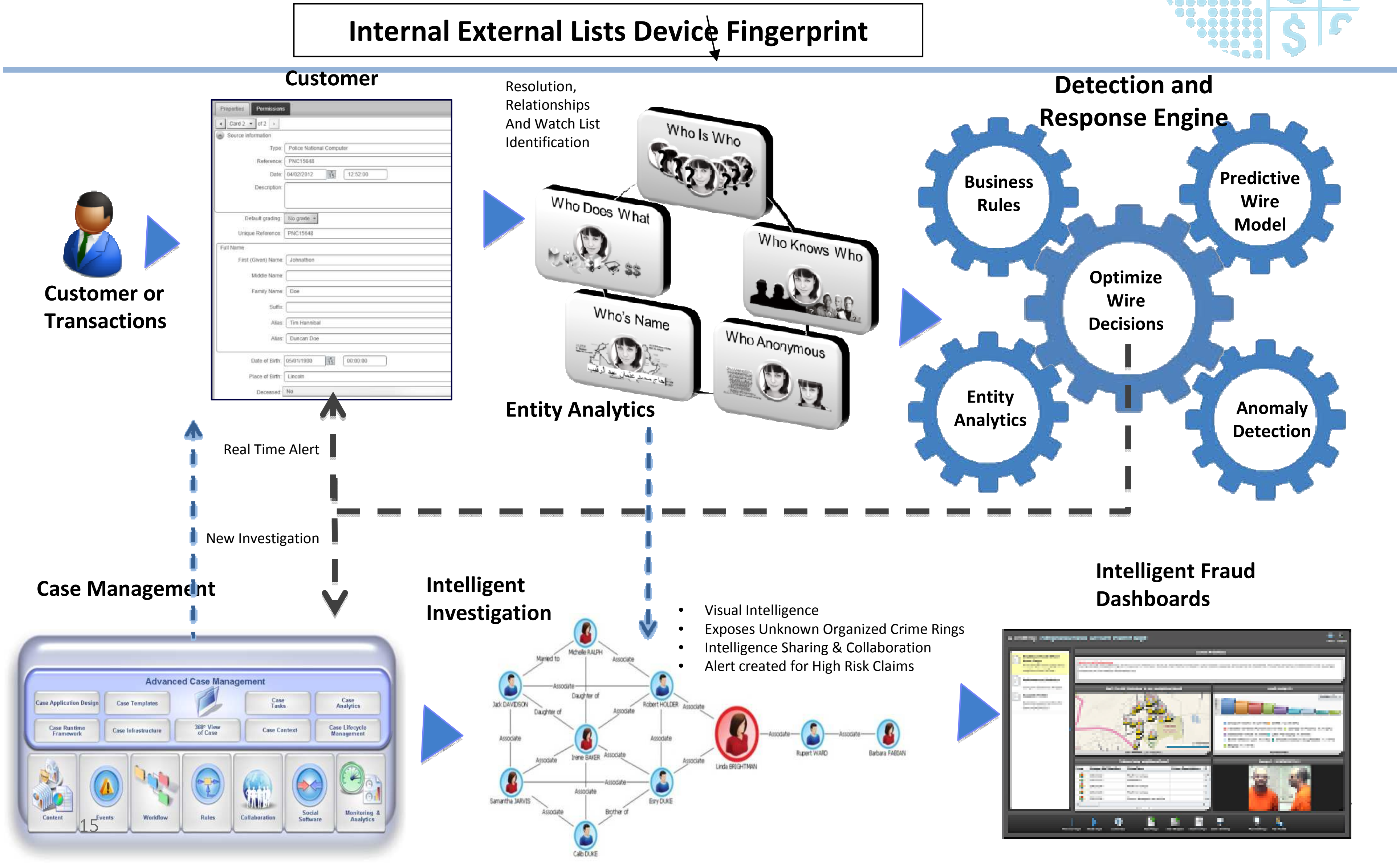
Content Analytics

GeoSpatial Analytics

Forensic Analysis

Social Network Analysis

Financial Crimes Scenario Walk through



Internal External Lists Device Fingerprint

Customer

Properties | Permissions

Card 2 of 2

Source information

Type:	Police National Computer
Reference:	PNC15648
Date:	04/02/2012 12:52:00
Description:	
Default grading:	No grade
Unique Reference:	PNC15648

Full Name

First (Given) Name:	Johnathon
Middle Name:	
Family Name:	Doe
Suffix:	
Alias:	Tim Hannibal
Alias:	Duncan Doe
Date of Birth:	05/01/1980 00:00:00
Place of Birth:	Lincoln
Deceased:	No

Customer or Transactions

Resolution,
Relationships
And Watch List
Identification

Entity Analytics

Detection and Response Engine

Business Rules

Predictive Wire Model

Optimize Wire Decisions

Entity Analytics

Anomaly Detection

Real Time Alert

New Investigation

Case Management

Intelligent Investigation

- Visual Intelligence
- Exposes Unknown Organized Crime Rings
- Intelligence Sharing & Collaboration
- Alert created for High Risk Claims

Intelligent Fraud Dashboards

MAY 10, 2013, 7:04 AM | 3 Comments

Daily Report: International A.T.M. Theft Takes $45 Million

By THE NEW YORK TIMES

- It was a huge bank heist — but a 21st-century version in which the robbers never wore ski masks, threatened a teller or set foot in a vault, Marc Santora reports in The New York Times.
- In two precision operations that involved people in more than two dozen countries acting in close coordination and with surgical precision, the organization was able to steal $45 million from thousands of A.T.M.'s in a matter of hours.
- In New York alone, the thieves responsible for A.T.M. withdrawals struck 2,904 machines over 10 hours on Feb. 19, withdrawing $2.4 million.
- On Thursday, federal prosecutors in Brooklyn unsealed an indictment charging eight members of the New York crew — including their suspected ringleader, who was found dead in the Dominican Republic on April 27 — offering a glimpse into what the authorities said was one of the most sophisticated and effective cybercrime attacks ever uncovered.
- "In the place of guns and masks, this cybercrime organization used laptops and the Internet," said Loretta E. Lynch, the United States attorney in Brooklyn. "Moving as swiftly as data over the Internet, the organization worked its way from the computer systems of international corporations to the streets of New York City, with the defendants fanning out across Manhattan to steal millions of dollars from hundreds of A.T.M.'s in a matter of hours."

Banks’ $1.6T secret

Laundering dirty $$

By JOHN AIDAN BYRNE

Last Updated: 12:05 AM, April 1, 2013

Posted: 10:43 PM, March 30, 2013

NEW YORK POST

Citigroup last week was just the tip of the iceberg — expect more major banks to be raked over the coals by regulators for lax controls in the hot $1.6 trillion money-laundering world, a top financial expert told The Post.

The Federal Reserve, Citi’s regulator, slapped the bank giant and the American branch of its Mexican affiliate, Banamex USA, on Tuesday over cracks in its detection processes for dirty money that’s laundered by criminals through the financial system.

But “Citibank is not alone,” international financial investigator L. Burke Files told The Post. “I am sure we will see warnings to JPMorgan Chase, US Bancorp, TD Bank, American Express, Bank of America and even HSBC before the year is out.

“They are not intentionally bad, they are just too big and remote from the risk,” said Files, a money-laundering expert who travels the globe cracking down on, and speaking about, multimillion-dollar fraud.

“Furthermore,” he added, “they are under economic pressures to lower costs and increase revenue, which means reducing staff and not upsetting the revenue cart.”

Compliance, meanwhile, is given short shrift in some quarters of the banking sector.

“Many of the banks will treat their compliance people like pariahs,” said Kieran Beer, editor-in-chief at the Association of Certified Anti-Money Laundering Specialists’ MoneyLaundering.com. “The businesspeople will think they are just a nuisance, getting in the way of making real money.”

Files says criminal gangs and financial fraudsters are gaming the banks. They know the soft touch. “Mr. Bad Guy wants to move a few million — just a few million. What does it take to buy or compromise a clerk making $60,000 per year to either subvert the system or just let them know what the bank’s KYC (Know Your Client) or EDD (enhanced due diligence) requirements might be? Once you have the bank’s checklist, you can game the bank.”

Tuesday marked the second embarrassing and costly rap for Citi in less than a year. The Office of the Comptroller of the Currency (OCC) hit Citi with a cease-and-desist order last April. The OCC called on the bank to ramp up its anti-money laundering controls.

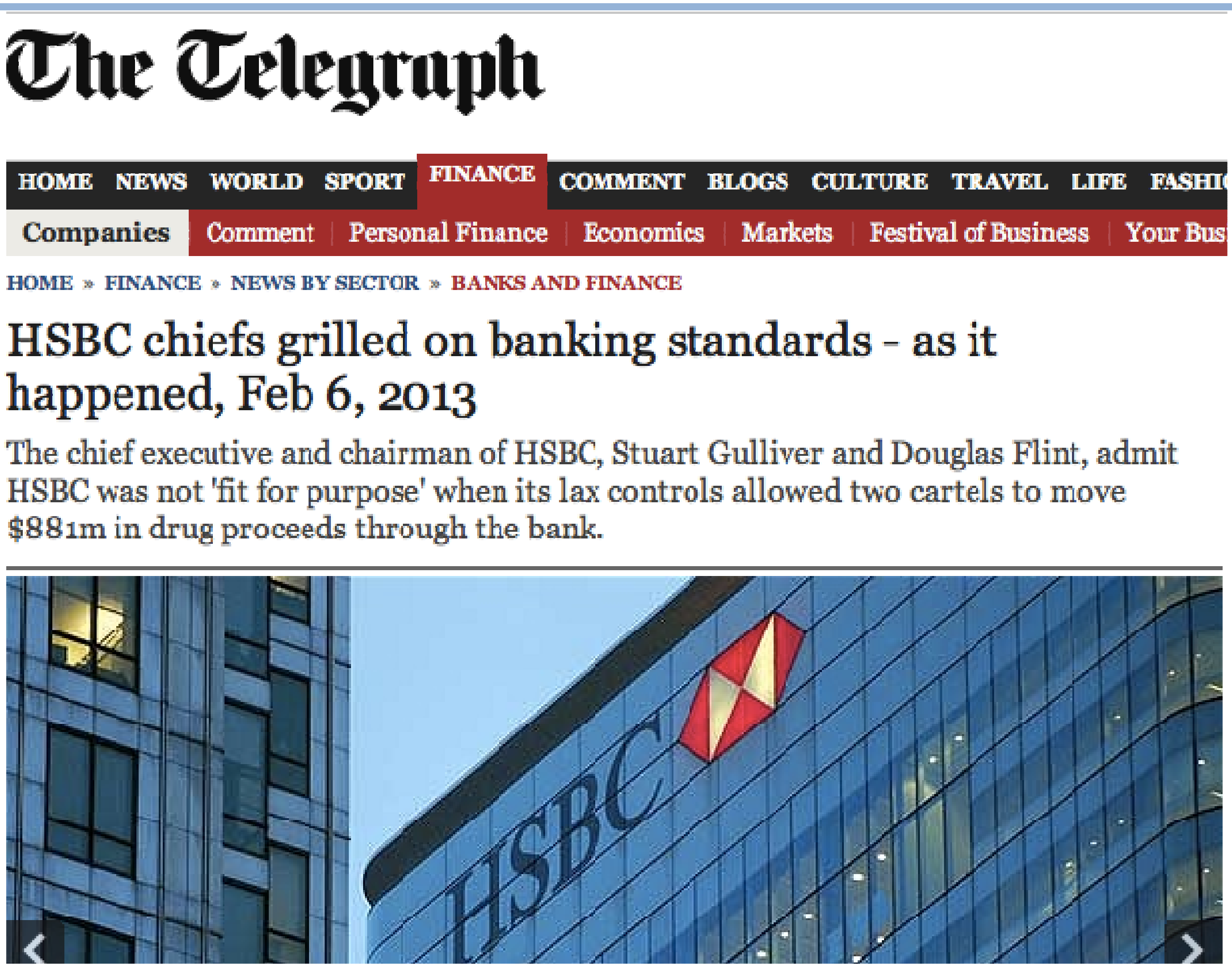
(In a separate case last December, HSBC was slapped in a record $1.92 billion deal with regulators, settling claims it moved billions of dollars for countries like Iran and empowered Mexican drug lords to transfer money illegally through the bank’s US affiliates.)

This latest time, the Federal Reserve blasted Citigroup for ineffective internal controls for overseeing suspicious money movements. And now it must embark on a program to plug the leaks. Although no fines were issued in the latest case, the program could cost Citi dearly — potentially hundreds of millions — through the hiring of more compliance staff, using expensive consultants and lawyers, and implementing new procedures to catch the money crooks, according to Beer.

Experts who spoke to The Post say money laundering in today’s high-tech financial markets has gotten more sophisticated since the events of 9/11 heightened concerns about terrorist and crime-fueled money transfers.

Six percent of cash flow in the US is the laundering of money, assuming the same percentage of the US economy is riddled with fraud and theft, says Files. Spending on anti-money laundering compliance will reach $5.8 billion this year, up from $5 billion in 2012, according to industry estimates. About $1.6 trillion is laundered worldwide, the most recently available rough calculations by the International Monetary Fund and United Nations indicate.

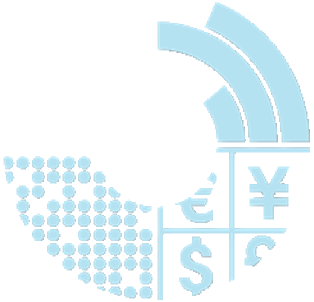
Britain's biggest bank was forced to pay $1.9bn (£1.17bn) fine to settle allegations by US regulators that it allowed itself to be used to launder billions of dollars for drug barons and potential terrorists for nearly a decade until 2010.


The Telegraph
HOME NEWS WORLD SPORT FINANCE COMMENT BLOGS CULTURE TRAVEL LIFE FASHI
Companies | Comment | Personal Finance | Economics | Markets | Festival of Business | Your Bus
HOME » FINANCE » NEWS BY SECTOR » BANKS AND FINANCE
HSBC

HSBC chiefs grilled on banking standards - as it happened, Feb 6, 2013

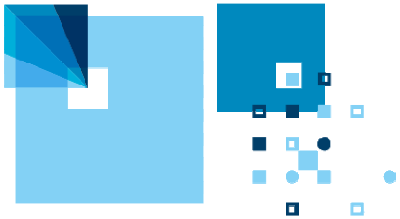
The chief executive and chairman of HSBC, Stuart Gulliver and Douglas Flint, admit HSBC was not 'fit for purpose' when its lax controls allowed two cartels to move $881m in drug proceeds through the bank.

Converging forces are creating a heightened focus on fraud and financial crimes



12 Cyber crime victims **per second**[1]

80% originate in organized activity[4]



Schemes are increasing in complexity and frequency

The explosion in global connectivity has escalated the vulnerabilities of individuals, enterprises and nations to cyber crime.

$4.7 **trillion** Global cost of fraud today[2]

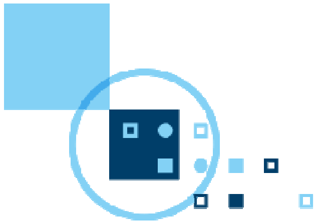
$1.92 billion fine in a money-laundering case[5]

Economic and societal costs of fraud have escalated

Intensified regulatory enforcement and operational losses apply significant pressure on profitability.

71% Customers who will switch banks because of fraud[3]

46% Customers leaving or avoiding a company with a security breach[6]



Customer expectations have intensified

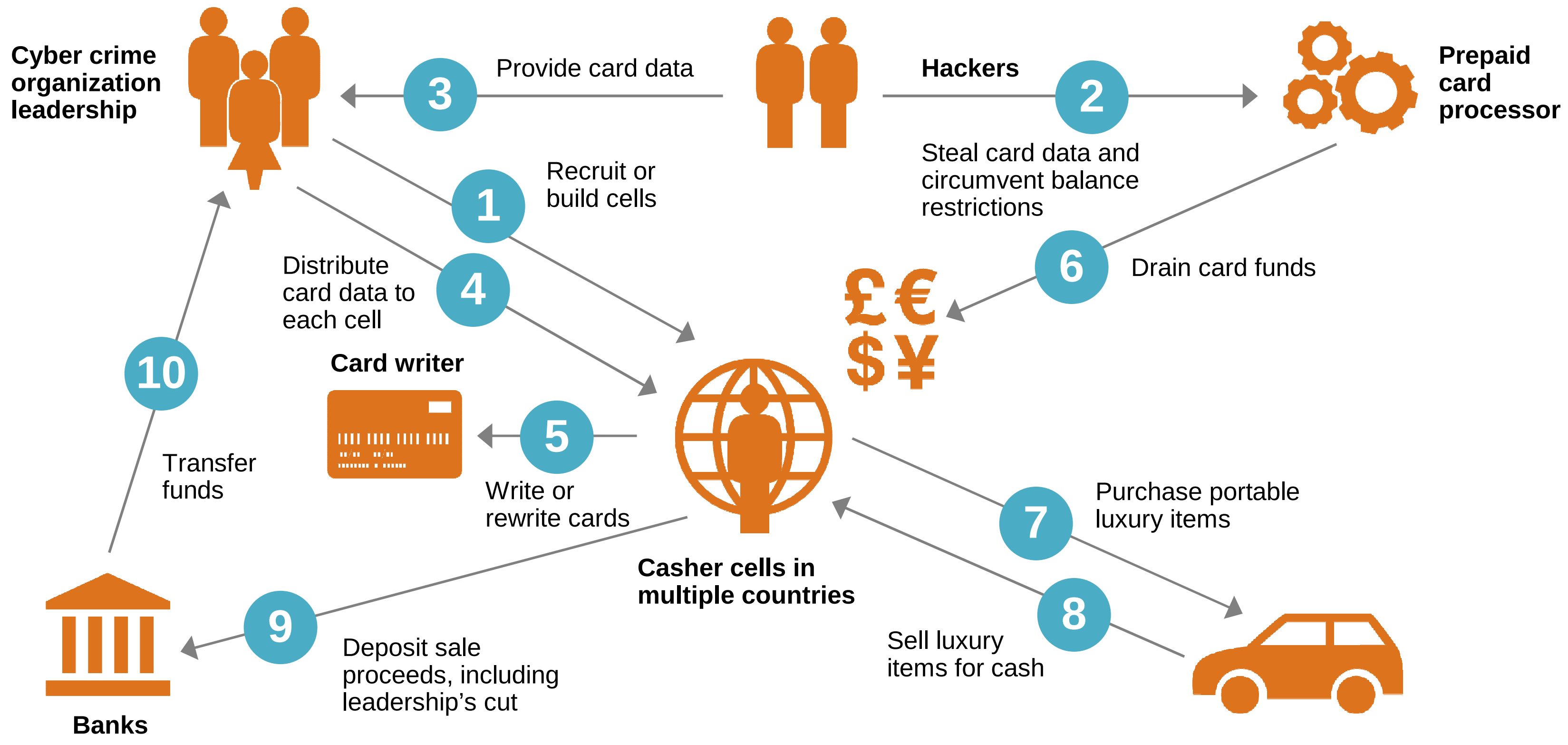
Customer confidence and trust drive brand choice and must be earned on an ongoing basis.

[1] 2013 Norton Report
[2] ACFE
[3] 2013 Harris Interactive
[4] 2013 Norton Report
[5] Reuters
[6] 2012 Edleman Survey

All amounts are in US dollars.

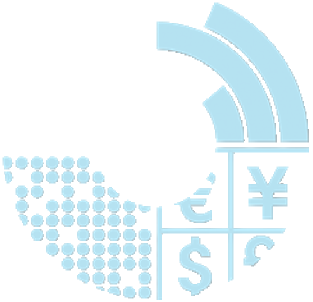
Schemes are increasingly complex, often involving networks of organized activity

Anatomy of a complex fraud scheme



Cyber crime organization leadership
3
Provide card data
Hackers
2
Prepaid card processor
Steal card data and circumvent balance restrictions
1
Recruit or build cells
Distribute card data to each cell
4
6
Drain card funds
£ €
$ ¥
10
Card writer
5
Write or rewrite cards
Transfer funds
Casher cells in multiple countries
7
Purchase portable luxury items
8
Sell luxury items for cash
9
Deposit sale proceeds, including leadership's cut
Banks

Proactively addressing this can translate into opportunity



Operational effectiveness

IBM client IBC reduced the time to detect a $1 million fraud ring by more than 99 percent from years to days[1]

- Loss avoidance
- Reduce false positives
- Focus investigations on high-risk cases to improve efficiency

Improved customer engagement

IBM client Santam delivered a 70 times faster settlement of legitimate claims[2]

- Deliver an optimal experience to legitimate customers
- Protect customer data
- Deter suspicious transactions with confidence

Brand value

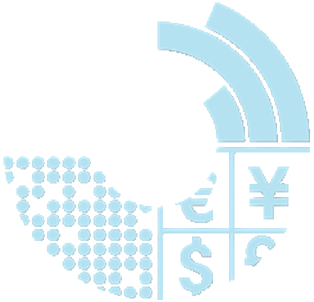
Reputation declines an average of $332 million as a result of an IT breach of customer data[1]

- Protect your brand reputation
- Engender trusted client relationships
- Support regulatory compliance obligations

[1] Ponemon Institute, *Reputation Impact of a Data Breach: U.S. Study of Executives & Managers*, November 2011.

All amounts are in US dollars.

Organizations continue to face challenges in capturing this opportunity



Internally, point solutions and corporate silo mentality contribute to increased risk of fraud and financial crimes:

•Analysts and investigators
•Claims
•Analytics
•Legal
•Risk
•Underwriting
•Management

The challenges:

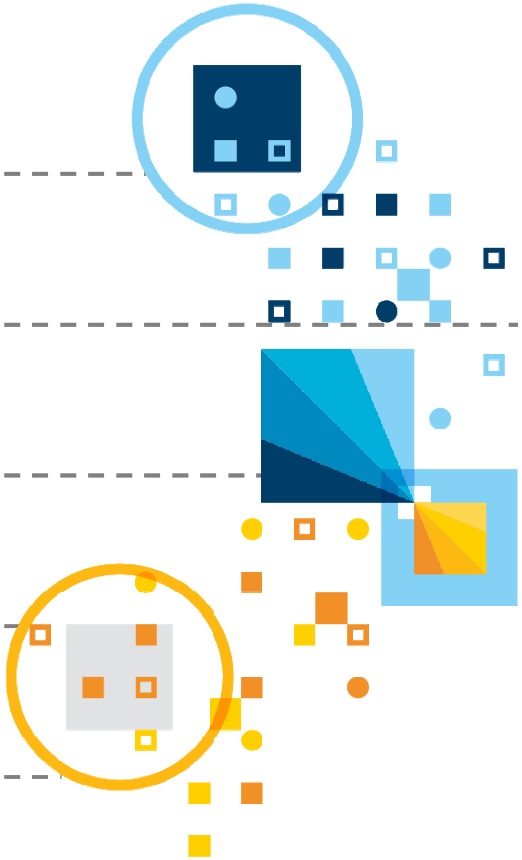
Prolonged action

High IT costs

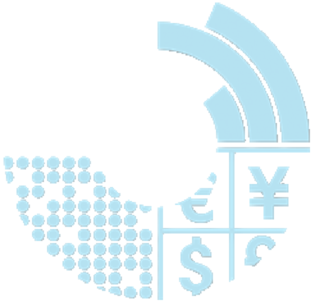
Transparency and compliance reporting are difficult

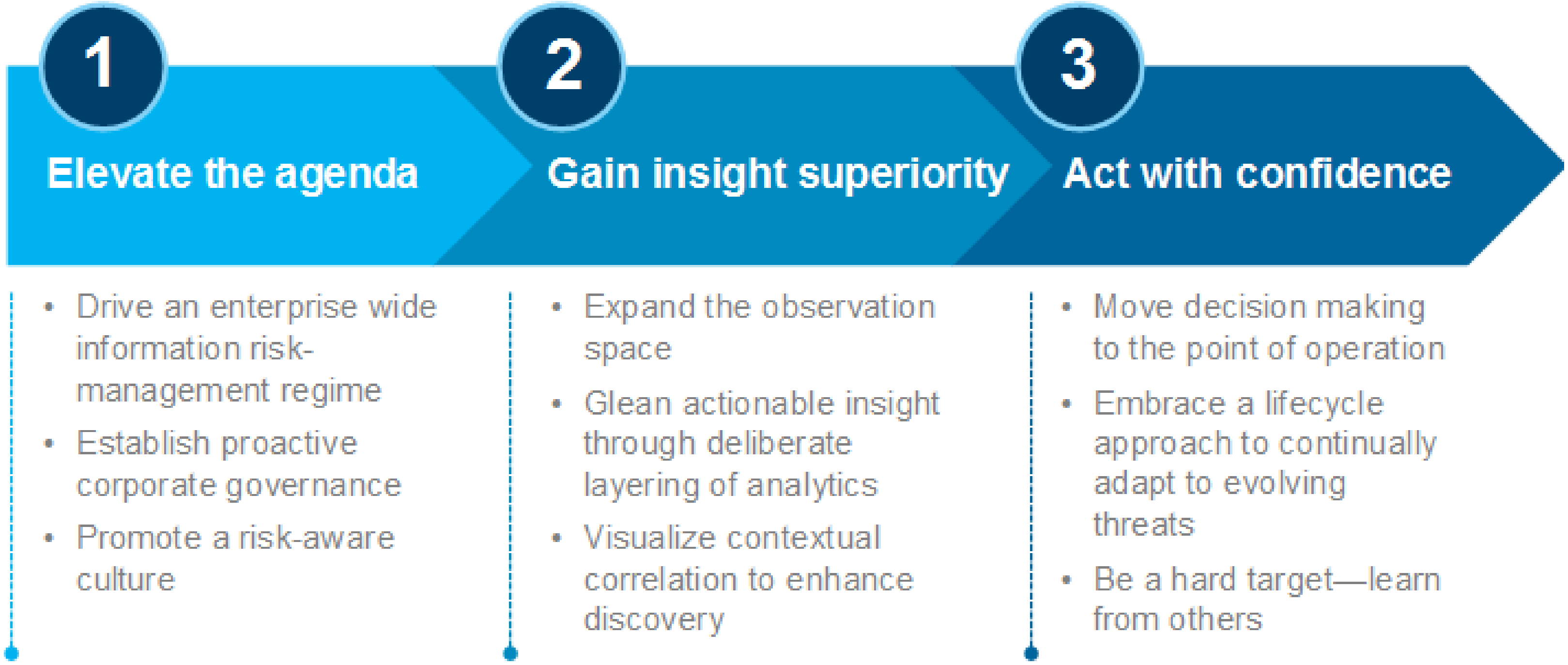
Fraudsters slip in through the gaps

Difficult to act nimbly to counter the threats



Forward-thinking leaders are adopting a strategic approach to countering fraud and financial crimes





1 Elevate the agenda

- Drive an enterprise wide information risk-management regime
- Establish proactive corporate governance
- Promote a risk-aware culture

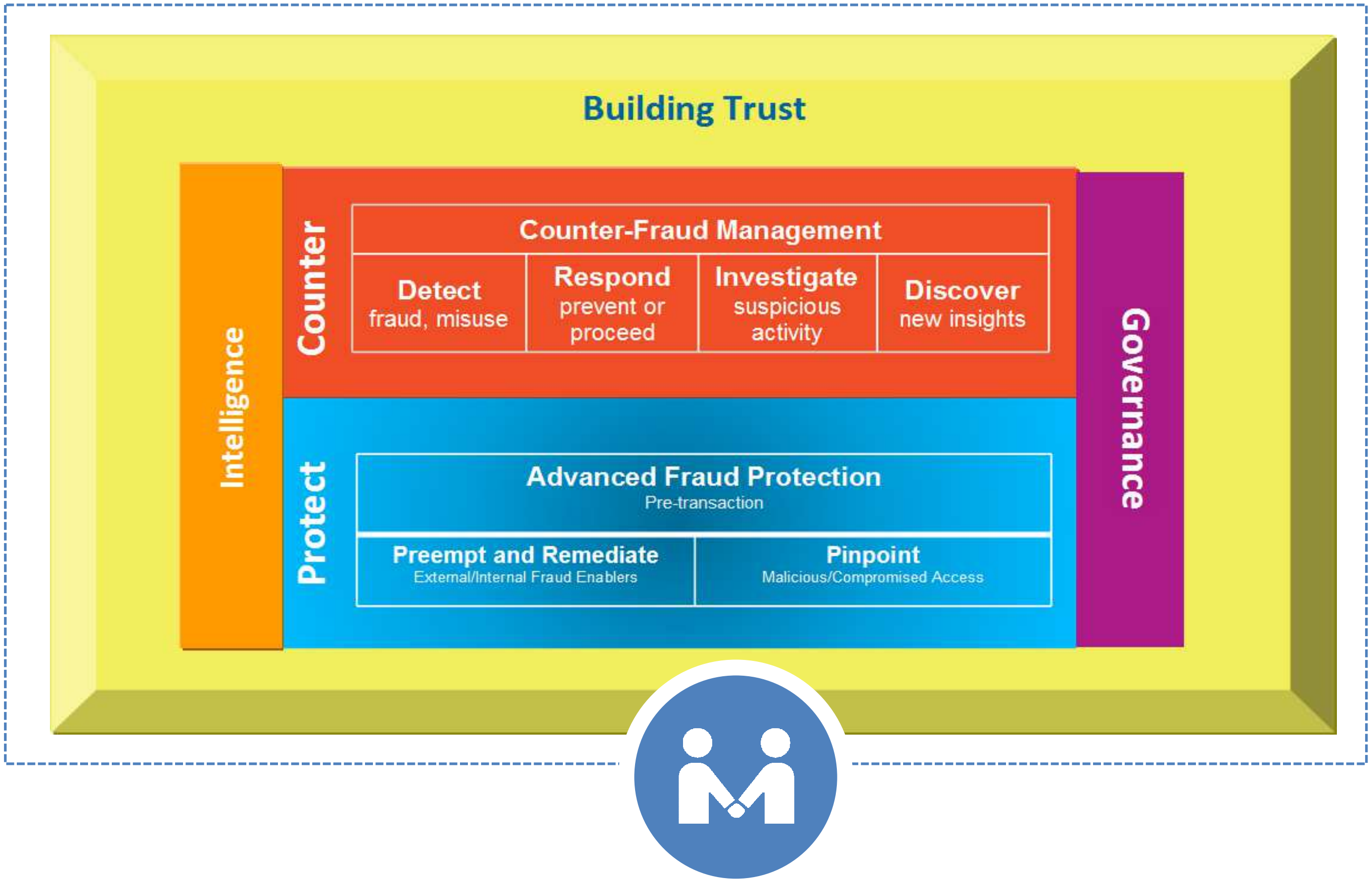
2 Gain insight superiority

- Expand the observation space
- Glean actionable insight through deliberate layering of analytics
- Visualize contextual correlation to enhance discovery

3 Act with confidence

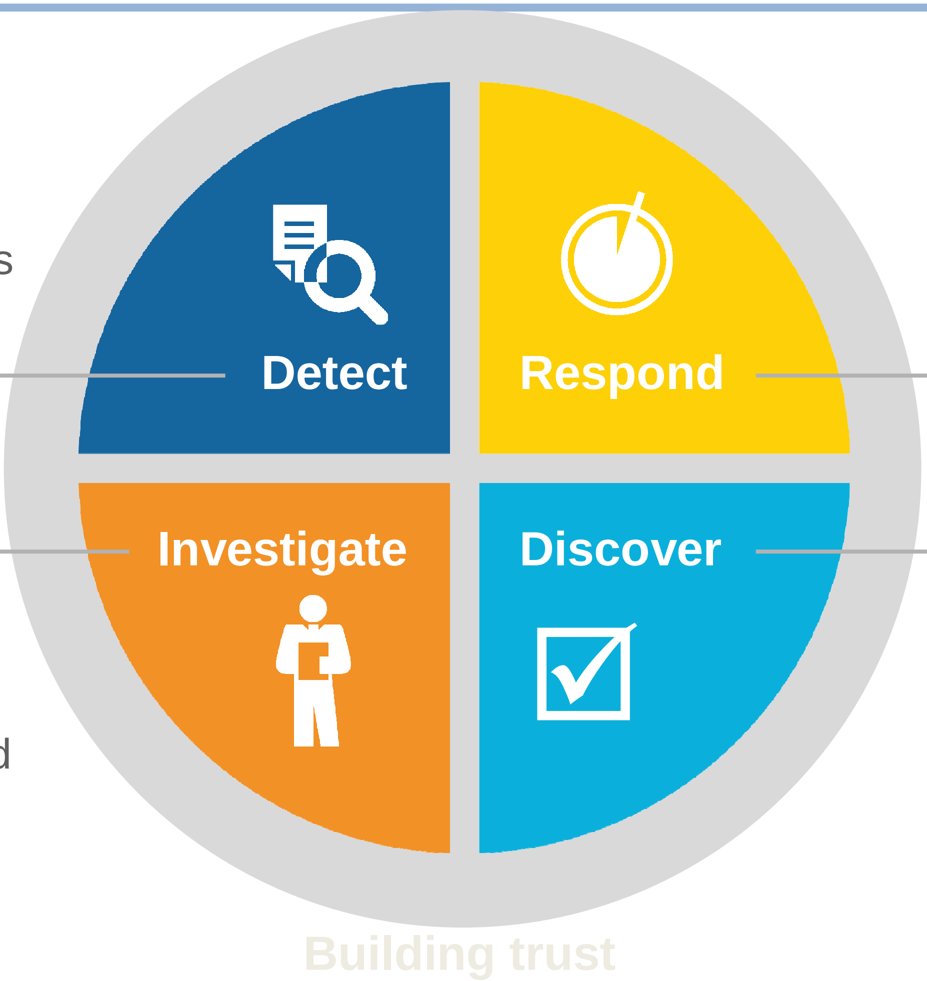
- Move decision making to the point of operation
- Embrace a lifecycle approach to continually adapt to evolving threats
- Be a hard target—learn from others

Counter Fraud Management helps organizations focus on the core initiatives that will build long term customer trust



Building trust

Counter-Fraud Management addresses each phase of an enterprise fraud approach



Detect fraud within a business process

Detect

Take action in real time—when it matters

Respond

Investigate

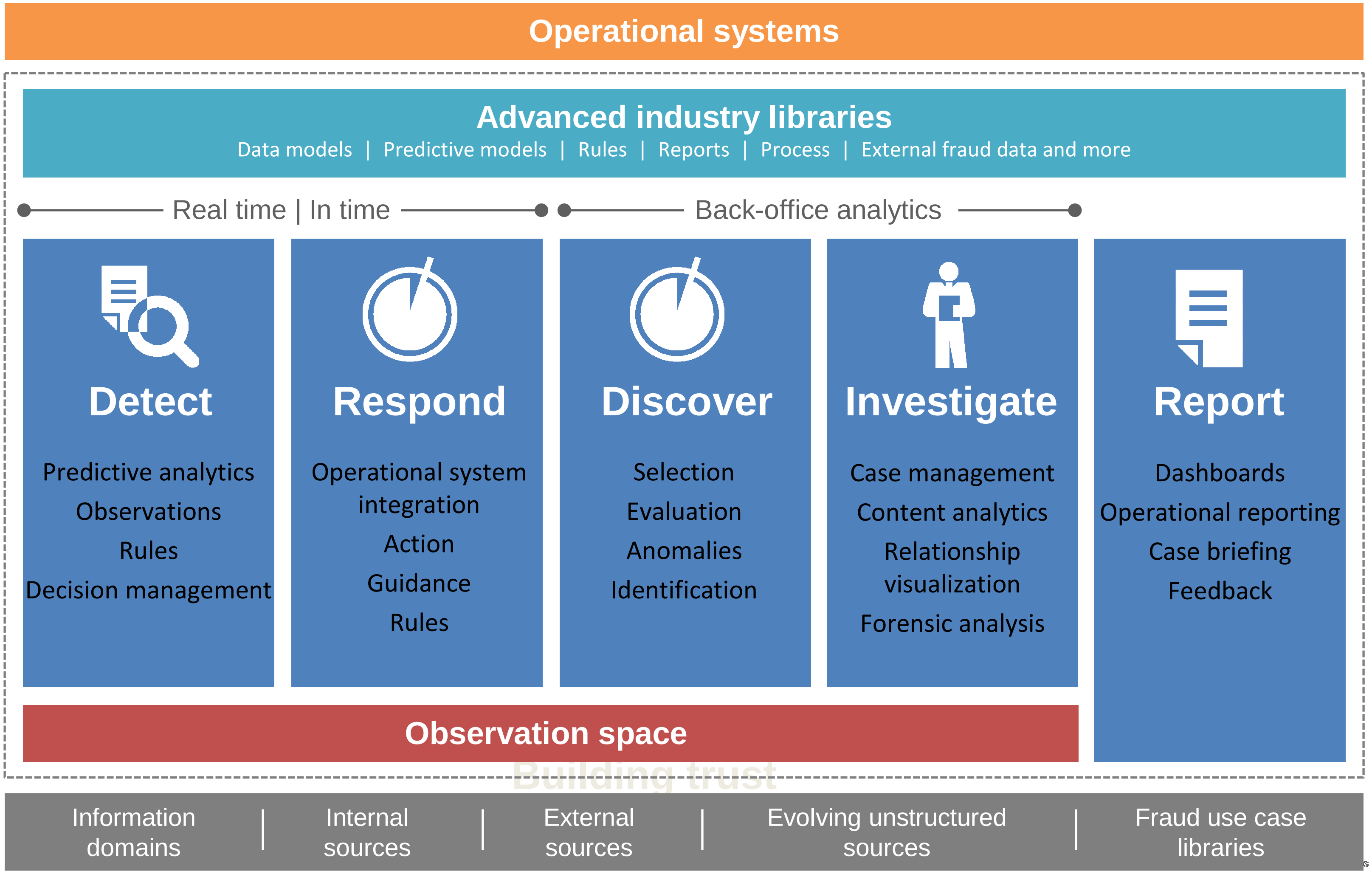
Confirm fraud for prosecution, recovery, rules and watch lists

Discover

Find fraud within the data

Building trust

Counter-Fraud Management offers distinctive and robust capabilities



Operational systems

Advanced industry libraries

Data models | Predictive models | Rules | Reports | Process | External fraud data and more

Real time | In time

Back-office analytics

Detect

Predictive analytics
Observations
Rules
Decision management

Respond

Operational system integration
Action
Guidance
Rules

Discover

Selection
Evaluation
Anomalies
Identification

Investigate

Case management
Content analytics
Relationship visualization
Forensic analysis

Report

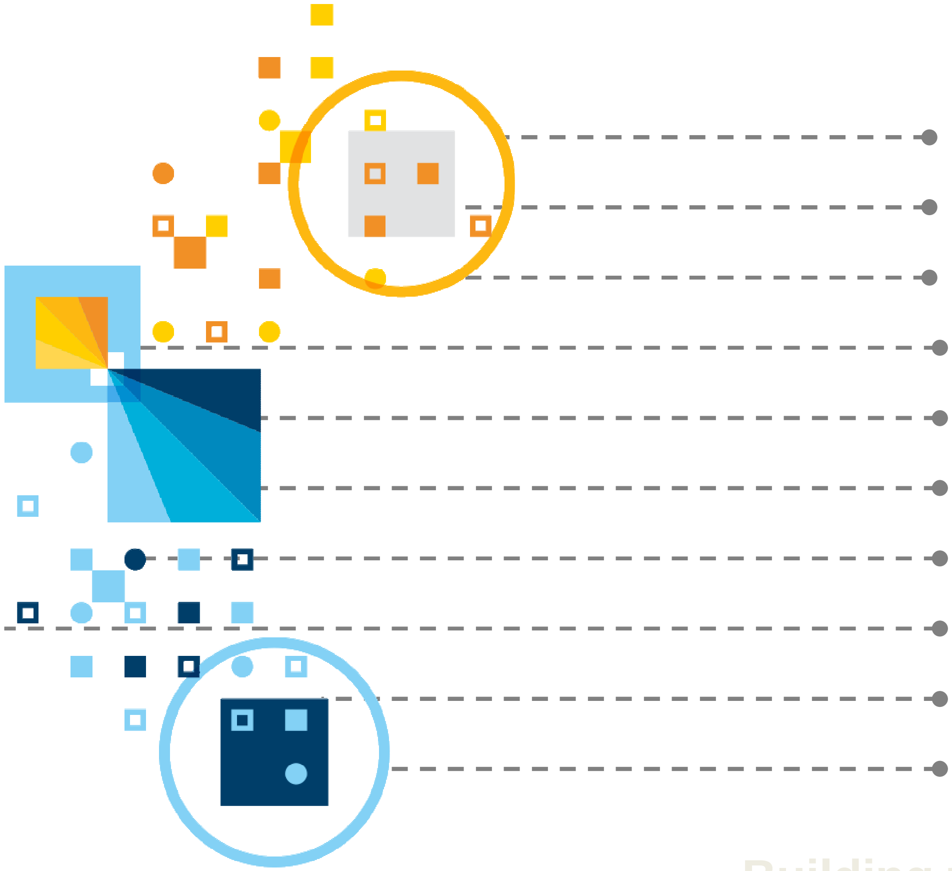
Dashboards
Operational reporting
Case briefing
Feedback

Observation space

Building trust

Information domains | Internal sources | External sources | Evolving unstructured sources | Fraud use case libraries

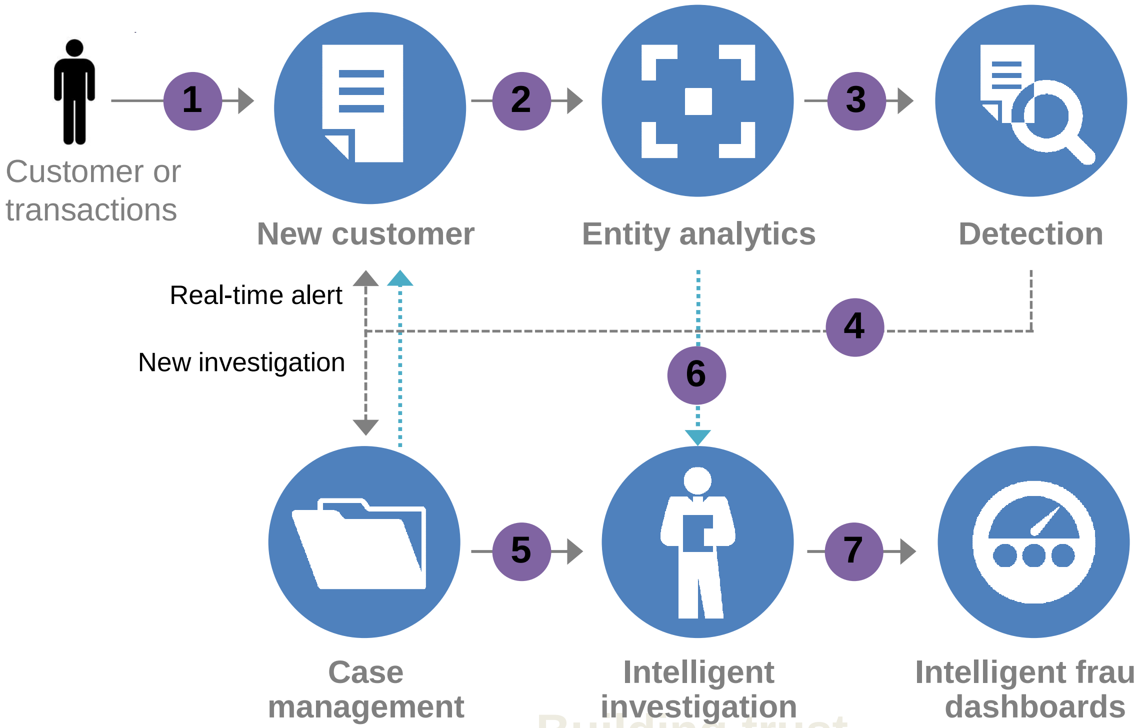
Counter-Fraud Management employs multilayered analytical techniques



- Entity analytics
- Predictive analytics
- Behavioral analytics
- Big data
- Context analytics
- Content analytics
- Decision management
- Geospatial analytics
- Forensic analysis
- Social network analysis

Building trust

Financial crimes scenario walk-through



Resolution, relationships and watch list identification

- Business rules
- Entity analytics
- Optimize wire decisions
- Predictive wire model
- Anomaly detection

Customer or transactions

1 New customer

2 Entity analytics

3 Detection

Real-time alert

New investigation

4

6

5 Case management

Intelligent investigation

7 Intelligent fraud dashboards

Fraud intelligent briefing and reporting

Building trust

- Visual intelligence
- Exposes unknown organized crime rings
- Intelligence sharing and collaboration
- Alert created for high-risk claims

Counter-Fraud Management solution enhance fraud and anti–money laundering operational effectiveness to support regulatory compliance

Business outcomes

Improved **suspicious transaction detection accuracy** through layering of deep analytic techniques to reduce false positives and false negatives

Enhanced **analyst and investigator productivity** by focusing on actual instances of fraud and facilitating an efficient collaborative investigation and case management process

Increased **operational effectiveness** without increasing staff

Confidence **in meeting regulatory compliance** obligations

80%

investigation productivity boost

40%

improved detection of suspicious transactions

Grupo Bancolombia uses data mining to identify potentially fraudulent transactions

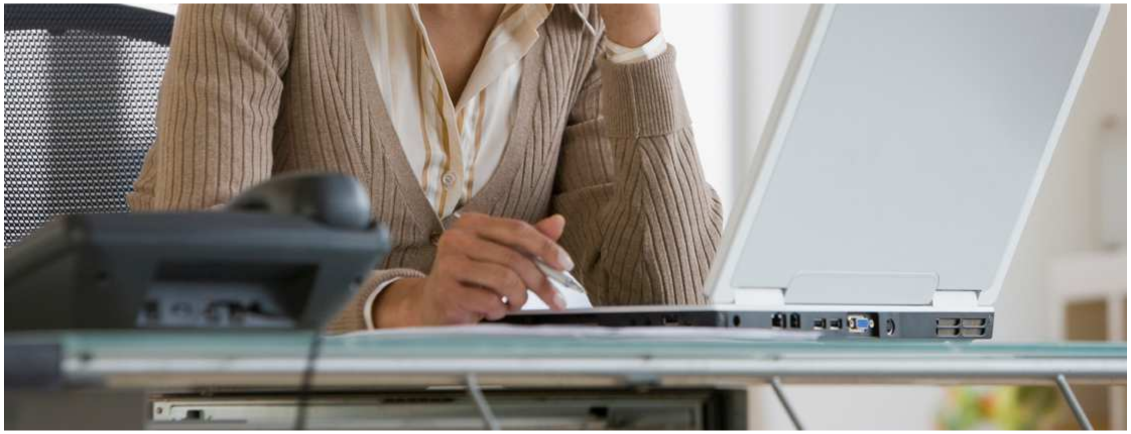
40%
increase in identifying suspicious transactions

200%
increase in reporting capabilities

80%
increase in analysis productivity

"With the data-mining system, we generated productivity savings of nearly 80 percent."

—Francisco Ruiz, head of compliance, Bancolumbia

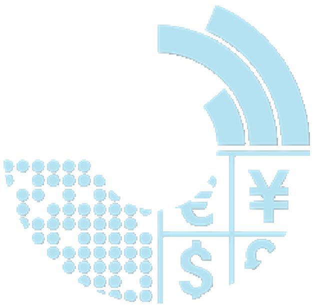


Business challenge: To adhere to stricter governmental reporting requirements, Grupo Bancolumbia needed to analyze millions of daily transactions to identify current and potential fraud.

The solution: The bank deployed predictive data-modeling software that helped it more easily and quickly detect transactions that were part of potential money-laundering operations. By detecting and analyzing expected and typical patterns of more than 1.3 million transactions a day, the solution prevents, detects and reports potentially fraudulent banking activities that may stem from criminals and terrorists.

Building trust

Why Counter- Fraud Management?



For smart organizations, fraud is not treated as a point solution or as a step in the process. It is more than a “score.” It starts before intake. It is seen as preventable, predictable and provable and is managed pervasively across the process lifecycle.

Collaboration

Drives transparency across users and provides guidance and alerts that improve smart decisions

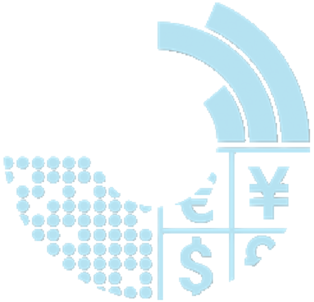
Multilayered

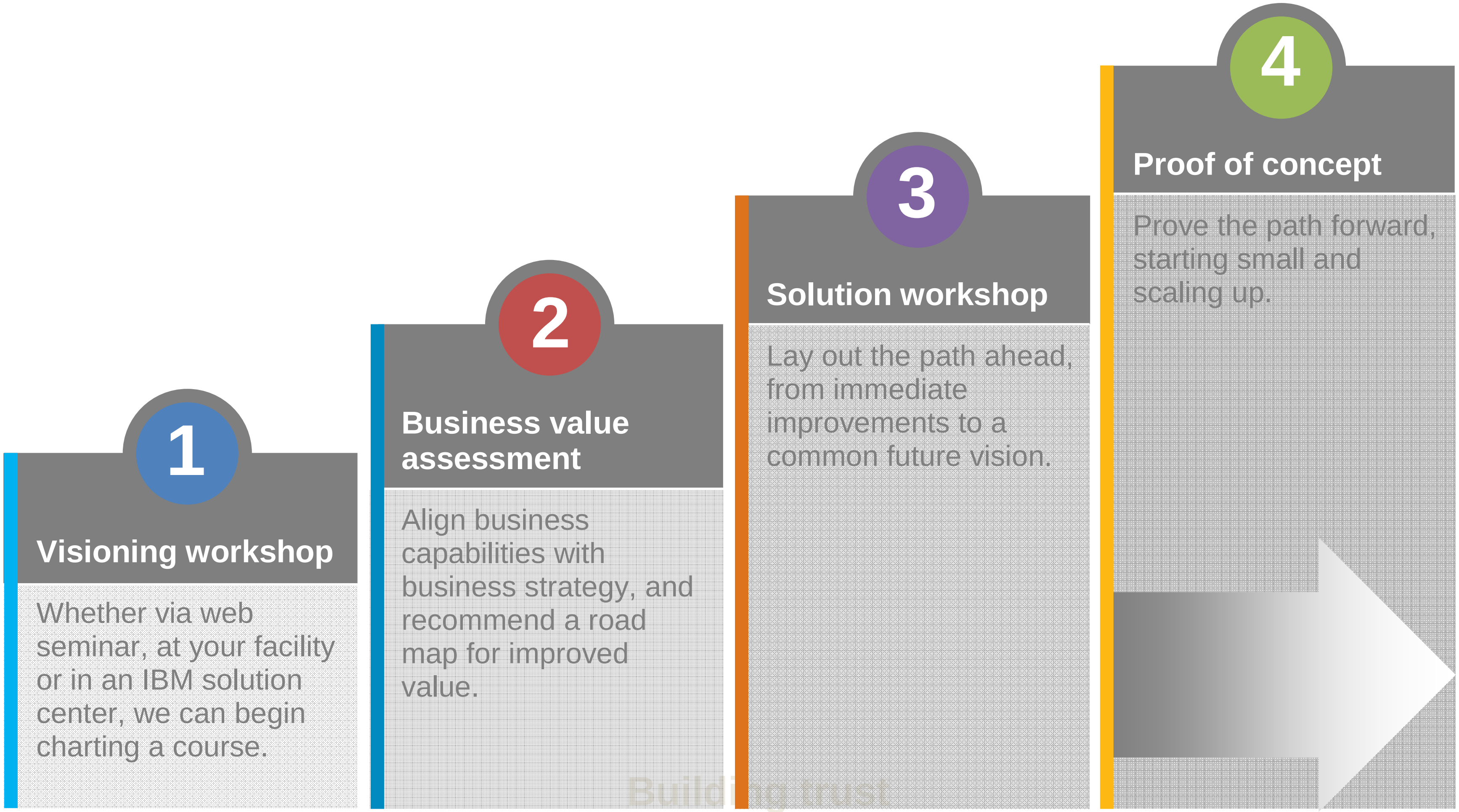
Considers a broad set of attributes, such as identity, relationships, behaviors, patterns, anomalies and visualization

Smart

Exhibits “smart” tendencies: it predicts, detects, discovers, manages, learns and more

Let’s get started achieving better business outcomes with proven approaches to collaborative problem solving





1 Visioning workshop

Whether via web seminar, at your facility or in an IBM solution center, we can begin charting a course.

2 Business value assessment

Align business capabilities with business strategy, and recommend a road map for improved value.

3 Solution workshop

Lay out the path ahead, from immediate improvements to a common future vision.

4 Proof of concept

Prove the path forward, starting small and scaling up.

Thank you!

Building trust