Operationalizing Integrity: A metrics-driven approach for universities

UC Regents – October 30, 2019

Building a better working world

Summary of today's agenda

- Operationalizing integrity – four key components
- Integrity analytics examples
- Deployment examples

Four components to operationalizing integrity

Reducing the gap between intentions and organizational behavior: that is the Integrity Agenda

From Intentions ...

- Mission and values statement
- Code of conduct
- Standards, policies and practices
- Management communications

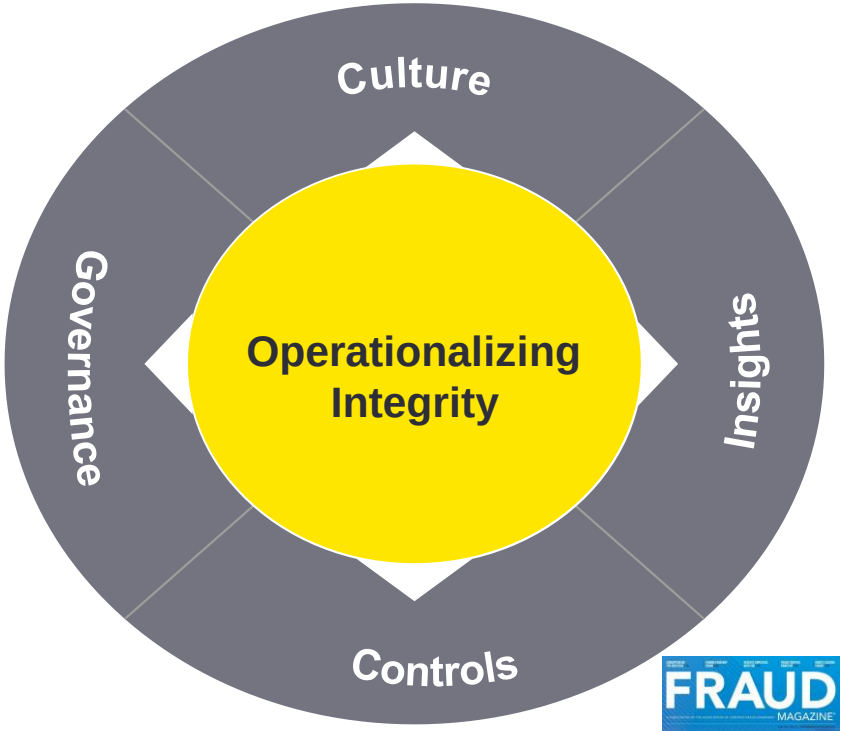
… to Actual Behavior

- Principles, behavioral standards and unwritten norms that guide employee and third parties actions
- Verifiable data about employee behavior and organizational culture
- Metrics

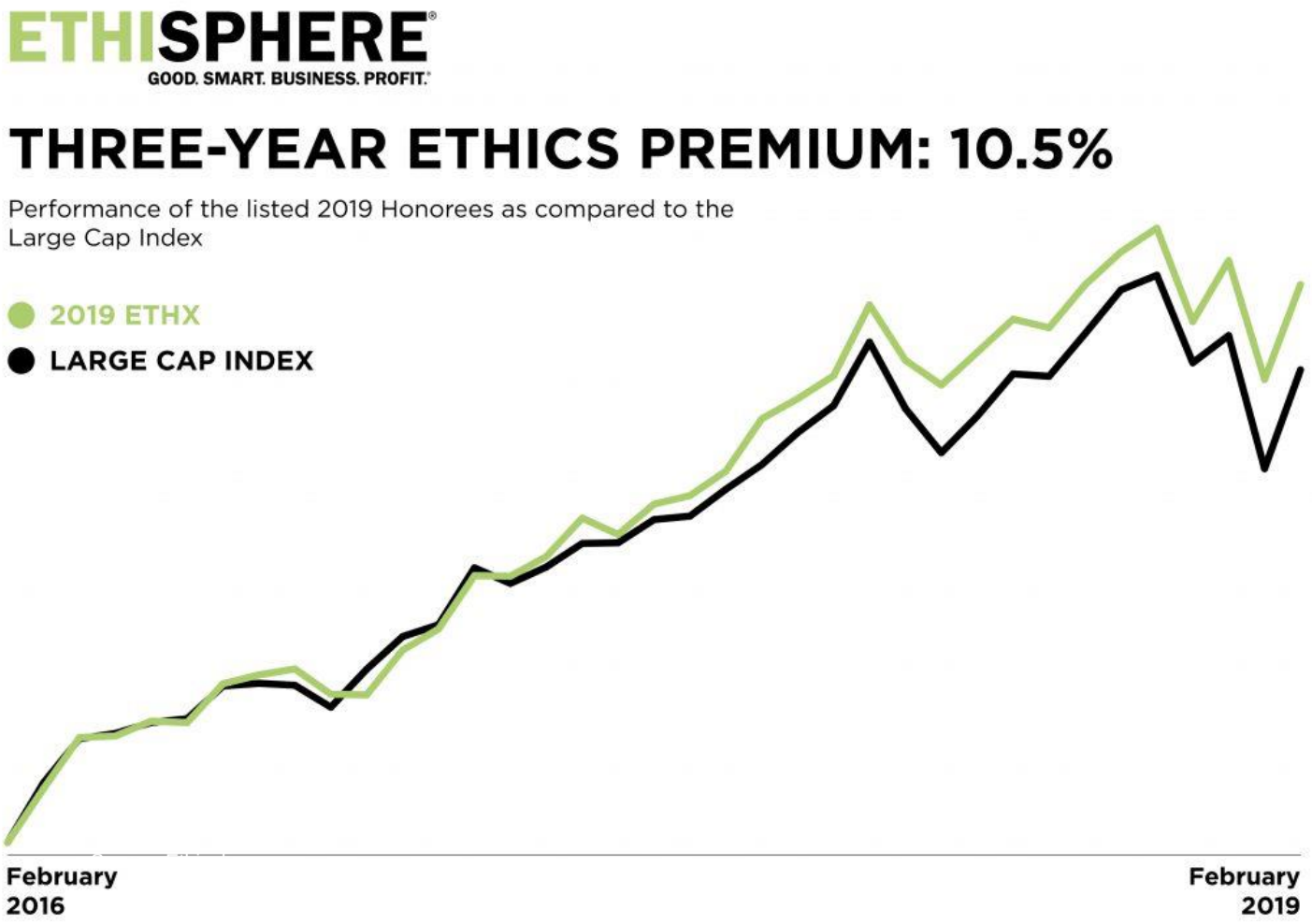
Key elements driving advanced analytics approach: operationalizing integrity that drive's transparency

Four key pillars of operationalizing integrity:

1. **Governance**: The structure of integrity management, encompassing board, line management and corporate functions, and the policies that guide organizational behavior.
2. **Culture**: The commitment to integrity that guides decisions across the extended enterprise. A culture of trust is vital for success.
3. **Controls**: Procedures that embed integrity into day-to-day operations, preventing and detecting violations of laws and policies
4. **Insights**: Data-based insights about emerging risks and integrity performance, driving program effectiveness and enriching employee knowledge.



"*What's your integrity agenda?*"
September/October cover issue of FRAUD Magazine


ETHISPHERE®
GOOD. SMART. BUSINESS. PROFIT.®
THREE-YEAR ETHICS PREMIUM: 10.5%
Performance of the listed 2019 Honorees as compared to the Large Cap Index
2019 ETHX
LARGE CAP INDEX
February 2016
February 2019

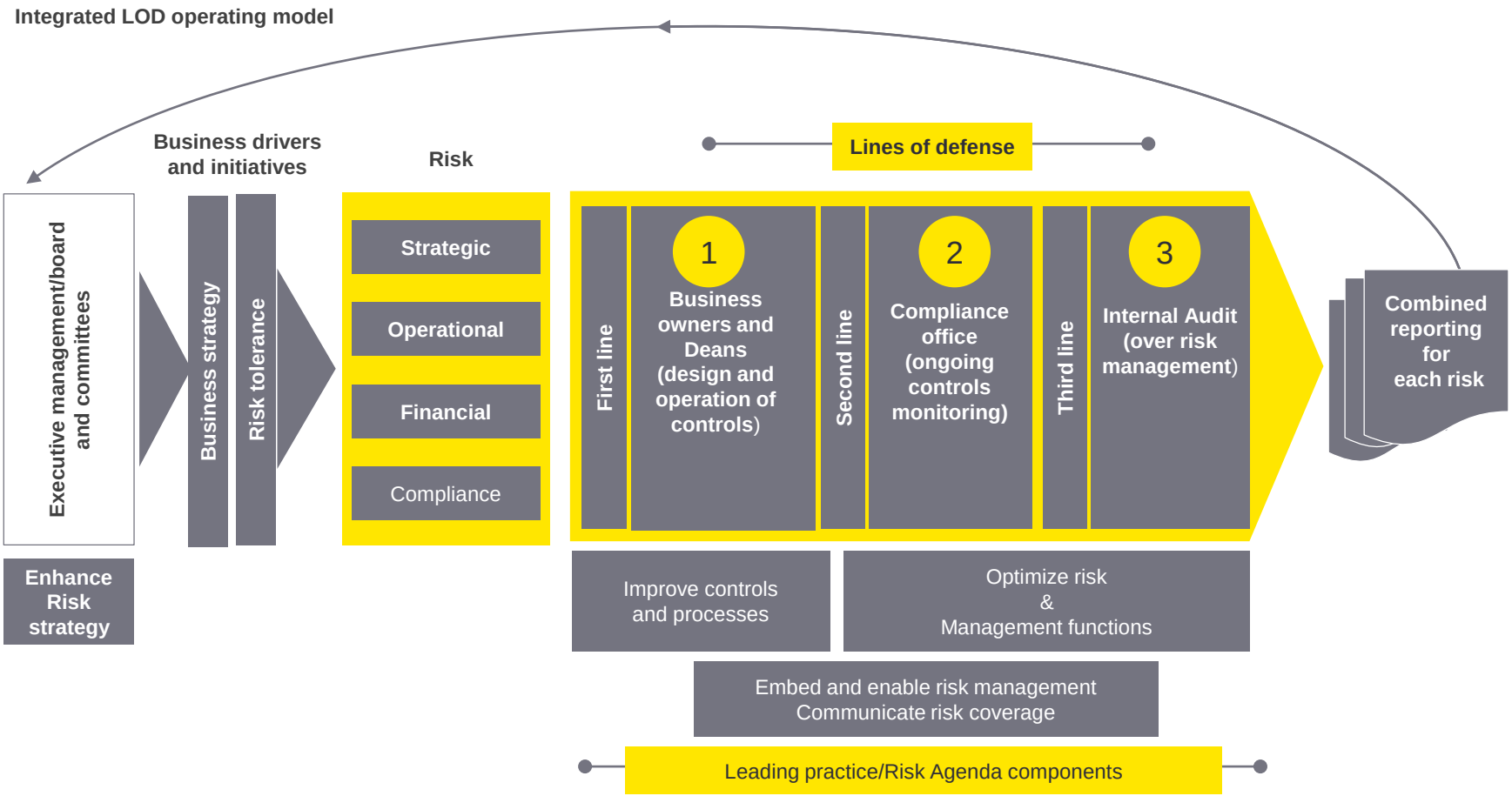
Corruption is #1 most common scheme in education
ACFE 2018 Report to the Nations

FIG. 16 **What are the most common occupational fraud schemes in various industries?**

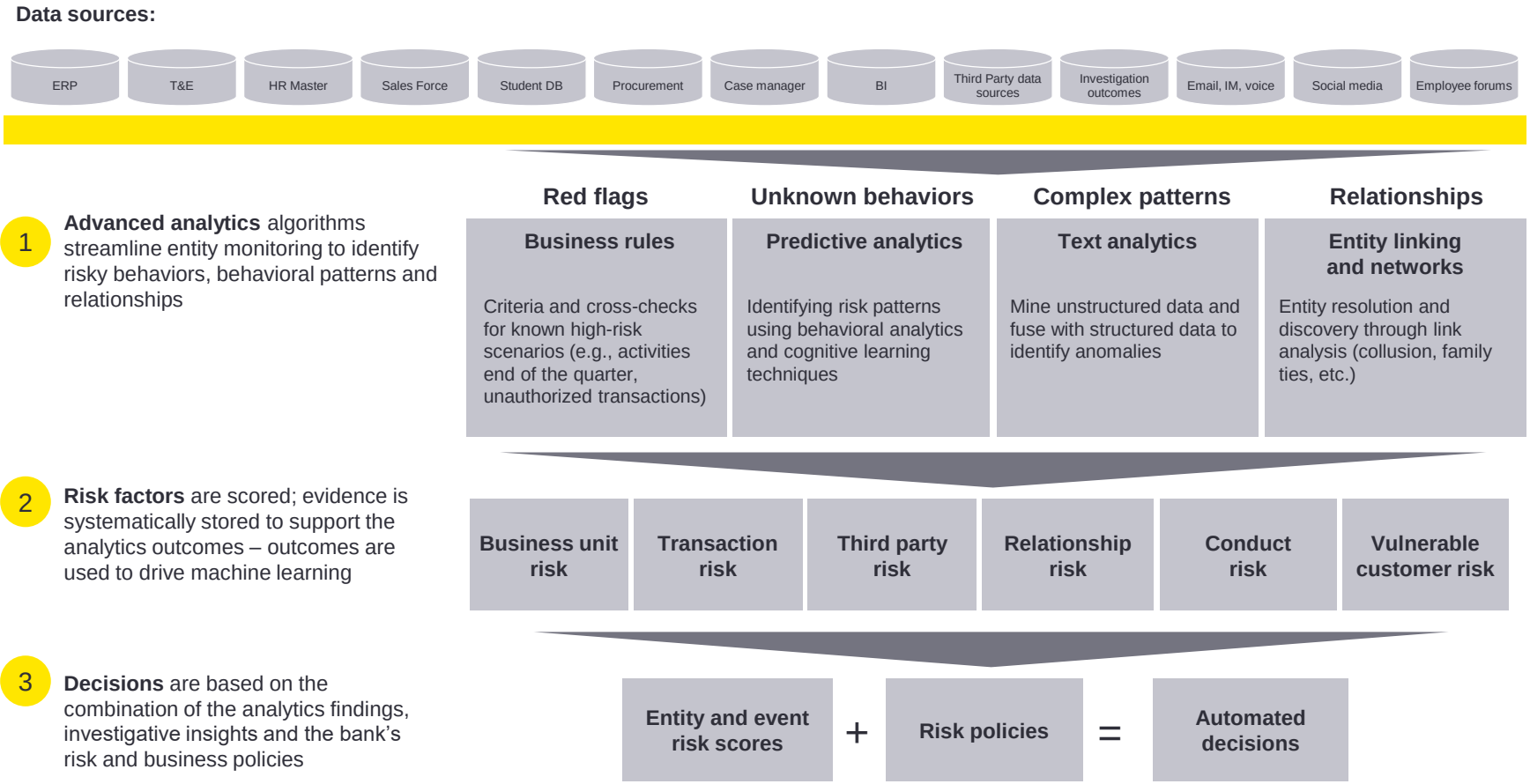
INDUSTRY	Cases	Billing	Cash larceny	Cash on hand	Check and payment tampering	Corruption	Expense reimbursements	Financial statement fraud	Noncash	Payroll	Register disbursements	Skimming
Banking and financial services	338	11%	14%	23%	12%	36%	7%	8%	11%	2%	3%	9%
Manufacturing	201	27%	8%	15%	12%	51%	18%	10%	28%	5%	3%	7%
Government and public administration	184	15%	11%	11%	9%	50%	11%	5%	22%	7%	2%	11%
Health care	149	26%	7%	13%	13%	36%	16%	11%	19%	17%	1%	12%
Retail	104	20%	10%	19%	9%	28%	8%	12%	34%	5%	13%	13%
Education	96	23%	19%	19%	6%	38%	18%	6%	19%	6%	0%	14%
Insurance	87	20%	9%	3%	18%	45%	8%	7%	11%	3%	1%	11%
Energy	86	20%	2%	10%	12%	53%	10%	3%	27%	7%	2%	10%
Construction	83	37%	12%	8%	19%	42%	23%	16%	23%	14%	1%	13%

Three lines of defense

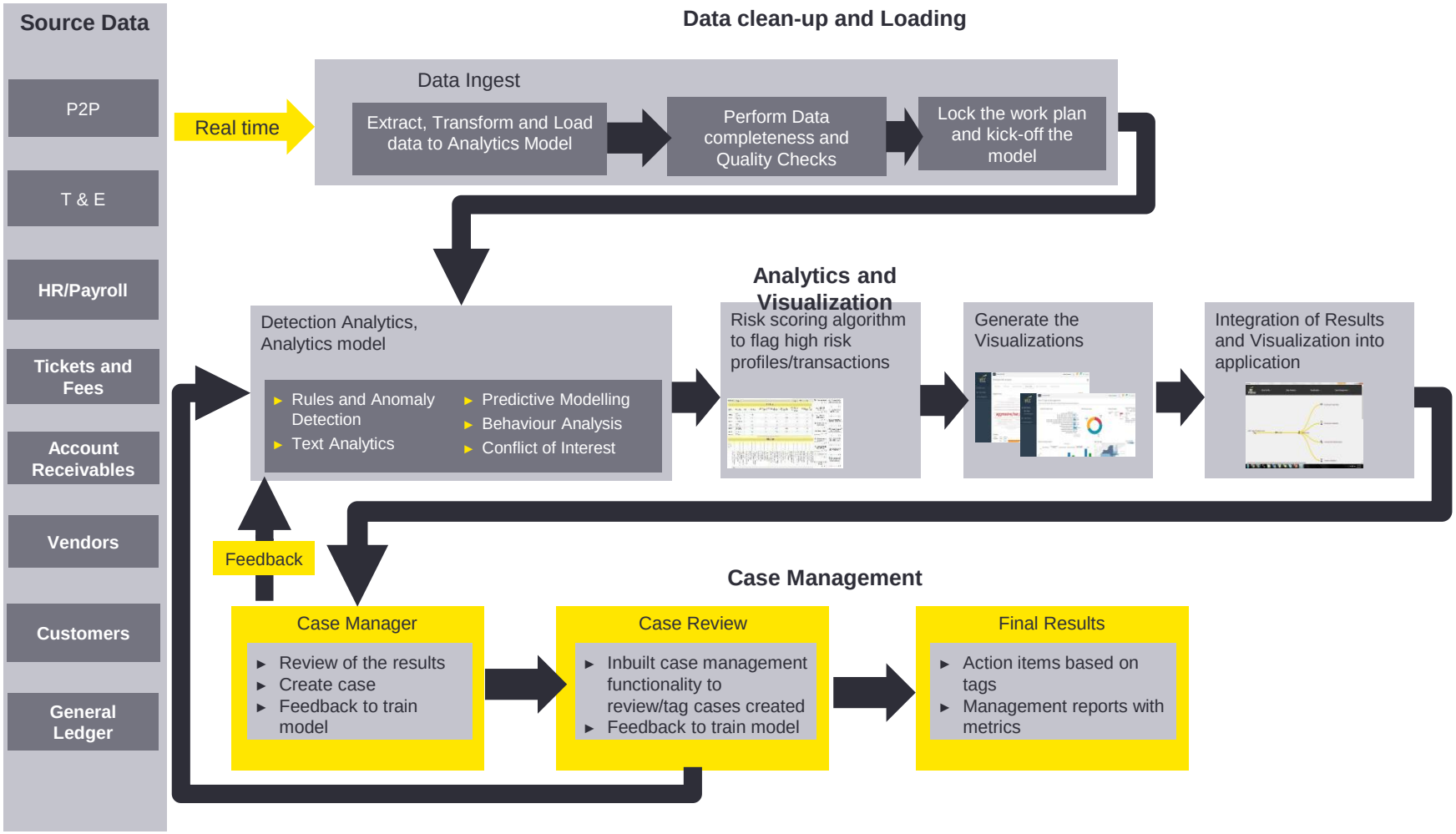
Compliance and IA's role in a 3 Lines of Defense Model



Integrity monitoring analytics – Conceptual Architecture



How it works – technical architecture



University integrity monitoring maturity example

Current State – compartmentalized

Current initiatives

- Purchase cards
- Grant programs
- Investigations
- Cost transfers
- Political contributions
- Travel and non-travel expenses
- Accounts payable

Future State – operationalized

New initiatives

- School financial operations
- Research – related parties and patent infringement
- Athletics finance review – fraud, waste and abuse
- Predicting student mental health needs
- Faculty grade changes
- Social media
- Faculty compensation time analysis for fraud, waste and abuse

Integrated risk scoring methodology

Limitations

- Ability to add new analytics and data sources is expensive and time taking
- Lack of executive reporting on overall compliance view and alerts management
- Lack of an integrated workflow and highly manual overall approach
- No ability to track and manage the review of high risk entities and transactions, as well as limited feedback into the model
- No presence of an automated verification system for vendors

Mature state

- Adoption of unified data model to risk score across departments
- Complete review platform with built-in case manager
- Triangulation of data sources
- Continuous monitoring for real or near time analytics
- Risk alerts
- University wide risk reporting, not just within different schools

Integrity analytics examples

University compliance analytics – example

Examples

University wide modules	Analytics across modules	Reporting
► Purchase cards ► Grant programs/Cost transfers ► Investigations ► Political contributions ► Accounts payable ► Disbursement Voucher – travel and non-travel expenses ► Donor data-Identifying quid pro quo arrangements	► Shared element testing, historical patterns, policy violations, circumvention of policies ► Statistical, text mining, visual mining, rules based testing, machine learning algorithms ► Predictive risk ranking model to risk rank transactions and entities	► University-wide reporting (across the schools) ► Intuitive and easy to understand visualization and reporting to help identify critical issues first. ► Drill down/roll up and dynamic risk scoring capability to assist with scenario modeling

Transaction Risk Ranking

Ey Pk	rank	Transaction Risk Score	T1: Government unallowable expenses	T6:Consistent expenses for meals / lodging above allowance per max rates	T7:Employees with consistent claim between $70 and $75 to avoid submi..	T9:Petty cash issued without SBO approval
2245	1	48.59	0.00	0.00	0.00	0.00
208828	1	48.59	0.00	0.00	0.00	0.00
200908	2	43.44	0.00	0.00	0.00	0.00
211640	2	43.44	0.00	0.00	0.00	0.00
24254	3	43.29	0.00	0.00	0.00	10.00
208477	4	39.97	0.00	0.00	0.00	0.00
200954	5	39.73	0.00	0.00	0.00	0.00
28887	6	39.39	0.00	0.00	0.00	0.00
58247	6	39.39	0.00	0.00	0.00	0.00
111442	6	39.39	0.00	0.00	0.00	0.00
153799	7	38.59	0.00	0.00	0.00	0.00
214594	8	38.35	0.00	0.00	0.00	0.00
214626	8	38.35	0.00	0.00	0.00	0.00
220653	9	37.65	0.00	0.00	0.00	0.00

Module example 1 – Cost transfers

- **Data Source –** General ledger data
- **Tests**

► Transactions where transaction date is within 30 days of Acct Exp. Date	► Accounts for transactions that deviate significantly from the normal range of volume and/or individual amounts
► Transactions where transaction date after Acct Exp Date	► Unusual foreign travel
► Round Dollar Transaction Amount	► Award budget utilization comparison between different schools and departments within 30 days of Acct Exp Date
► Duplicate Transactions with Different object code and Amount	► Award budget utilization comparison between different schools and departments within first 30 days of Acct Eff Date
► High Dollar low frequency	► Unusual Administrative expenses
► Low Dollar High frequency	► Unusual Miscellaneous expenses
► Fraud keyword's test analytics on name and description fields	► Unusual Interdepartmental transfers
► Duplicate Transactions with Different Amount	► Unusual Electronic equipment
► Analysis of potential reversals	► Unusual Expenses of meals
► Sudden increase in # of transactions in one period compared to another	► Write-offs to advance accounts or other prepaid asset accounts

Module example 2 – Accounts Payable

- **Data Source –** Account payables, Purchase orders and Vendor master
- **Tests**

► Keyword search of payment descriptions for keyword terms related to licensing and permit activities	► Round dollar Invoices (Threshold Amount $100)
► GL accounts for licensing or permit expenses	► Invoiced and paid on the same day (Threshold amount >$1,000)
► Keyword search of payment descriptions for keyword terms related to customs	► Duplicate invoices that have same date, same invoice number and same amount for same vendor
► GL account for customs clearance expenses	► Duplicate invoices that have same date, same invoice number and same amount for same payment vendor
► Duplicate payments: payments made for the same amount, to the same vendors/distributors, and/or with the same invoice number	► Duplicate Invoices that have the same date, invoice number and amount for different vendor
► Vendors matching with employee same/similar name	► Duplicate payments that have the same date, invoice number and amount for different payment vendor
► Vendors matching with employee same/similar street address	► Duplicate Invoices that have the same date, amount and vendor with a similar invoice number
► Vendors matching with employee same/similar Mailing address	► Duplicate payments that have the same date, amount and vendor with a similar invoice number
► Vendors and Employee matching with same Phone Number	► Split payment analysis where payment amount is greater than 0
► Payments made to Employees after they were terminated/resigned (after 90 days)	► Identify Invoices where Payment amount is greater than Invoice Amount
► Payment using one-time vendor codes	► Identify monthly recurring payments (greater than 3 months) where amount is greater than $1,000
► Payments made to vendors or distributors not listed in the vendor/distributor master files	► Identify outlier and unusual payments using statistical anomaly detection by vendor

Module example 3: Student-centric compliance analytics (“SCA”)

Overview

Transforming the compliance field using advanced and predictive analytics

Student

- Training
- Attendance
- Medical Records
- USCard

- Grades
- Student information
- Student hotline data
- Social media

Analytics

Based on research co-developed with GE on “digital twins”.

INNOVATION UPDATE

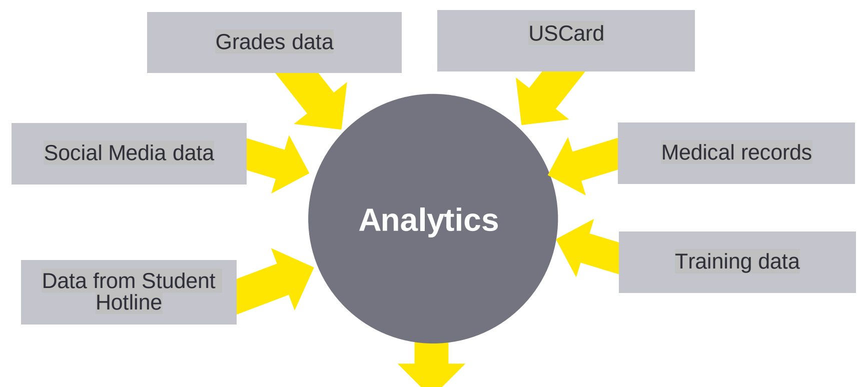
‘Profit & Loss-of-One’

Preventing fraud, enhancing compliance using digital twins

Scope

Proactive data analytics will help educational institutes by providing insights that would help in better decision-making capabilities. It can help the institutes offer personalized education, identify alarming student behaviour and support monetary decisions.

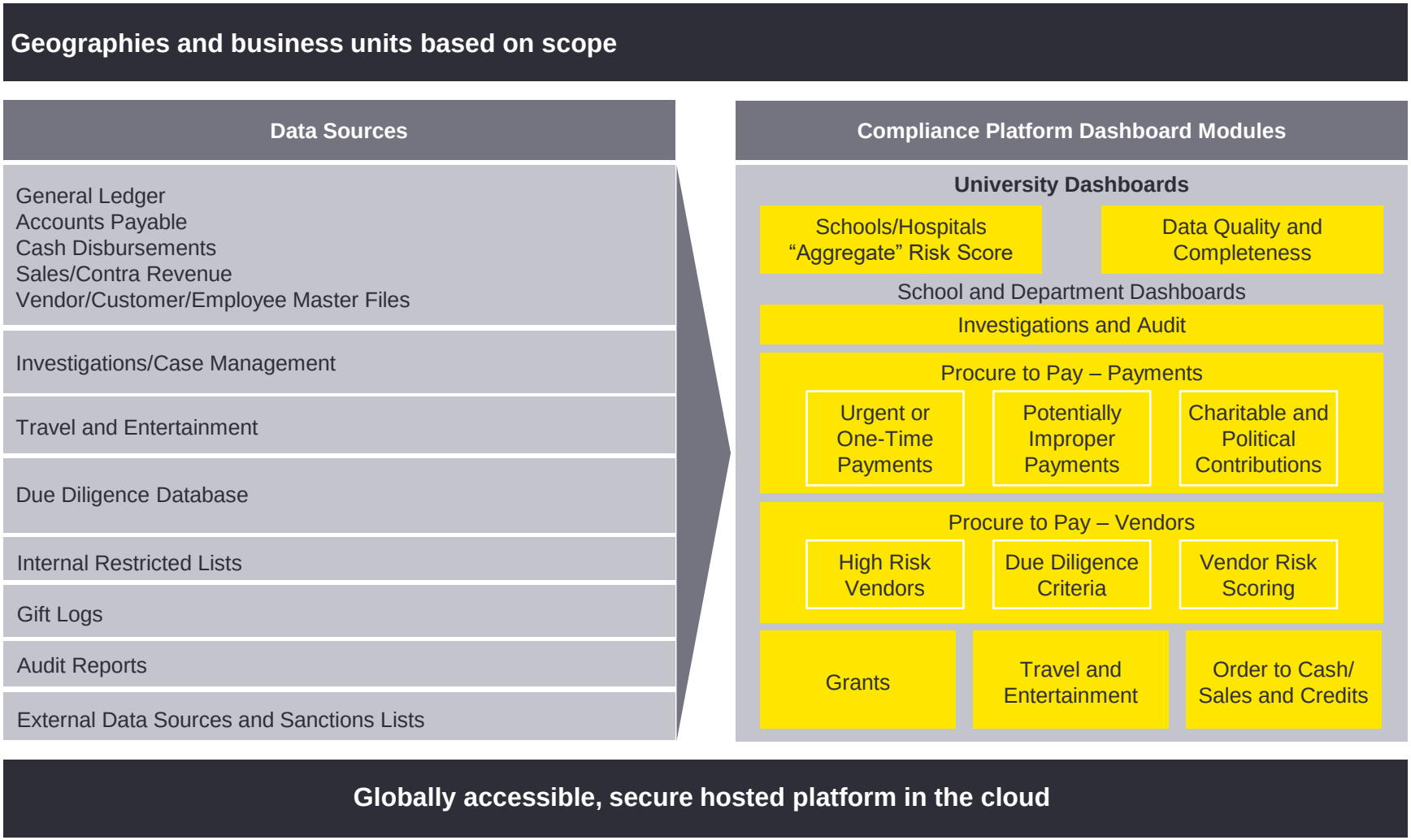
- Collect data of students
- Identify risk based on alarming messages on social media/other data sources
- Pull data from multiple data sources to build analytics
- Based on risk trigger, patterns identified, etc. the communication approach was defined



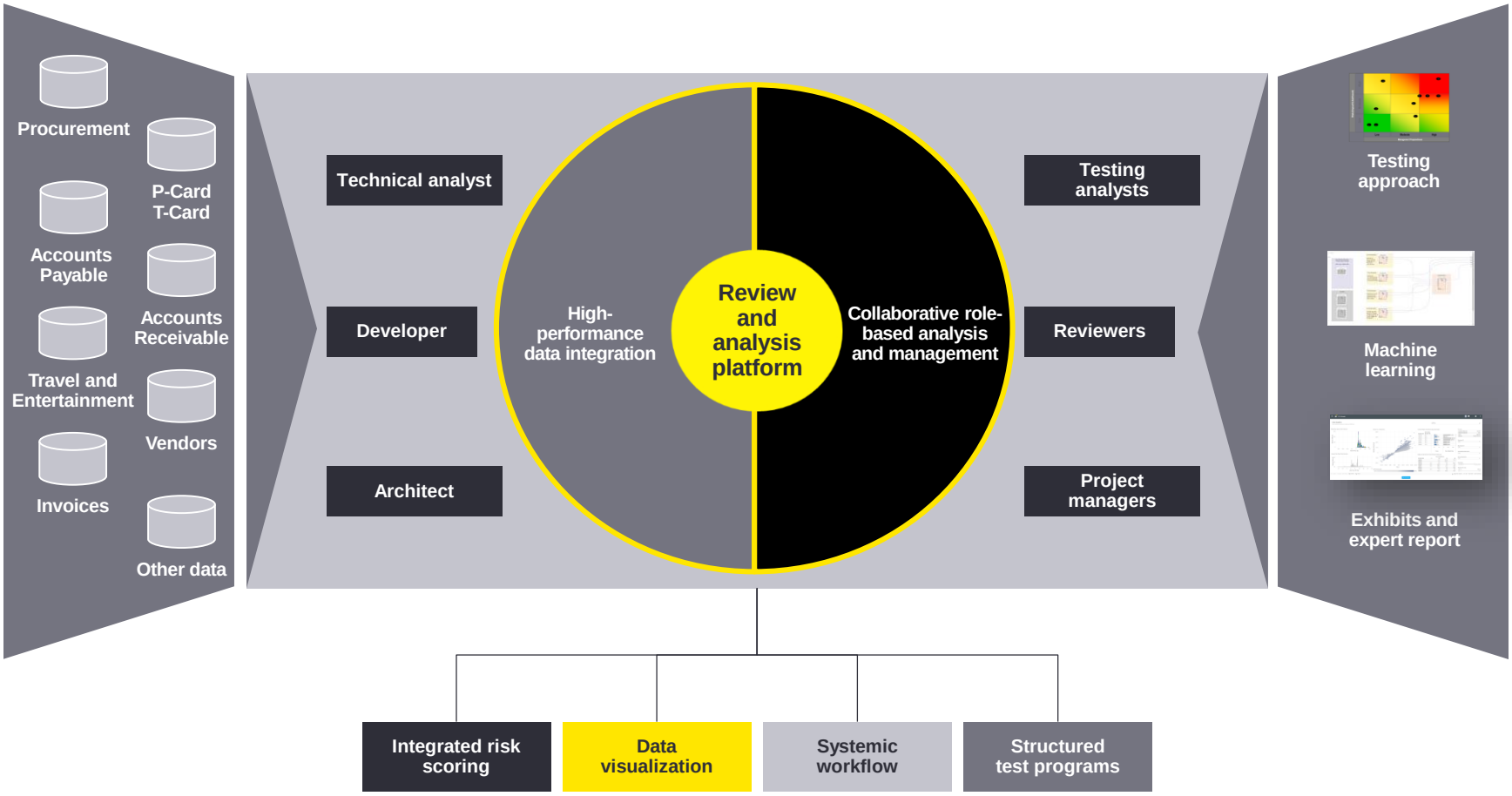
Automated, intriguing and relevant (AIR) communications

Deployment considerations

Asking more robust, better questions with a unified data model



Easy-to-use, integrated platform that drives transparency



Assemble multiple, disparate data sources into a single view for testing and analysis that support internal and external decision making

Five key questions – before you jump in

- What are our most significant ethics and compliance risks at our University?
  - What are they and in what schools?
- Who is accountable for managing them?
- What are they doing?
- Is it working?
- How do we know?

Q&A

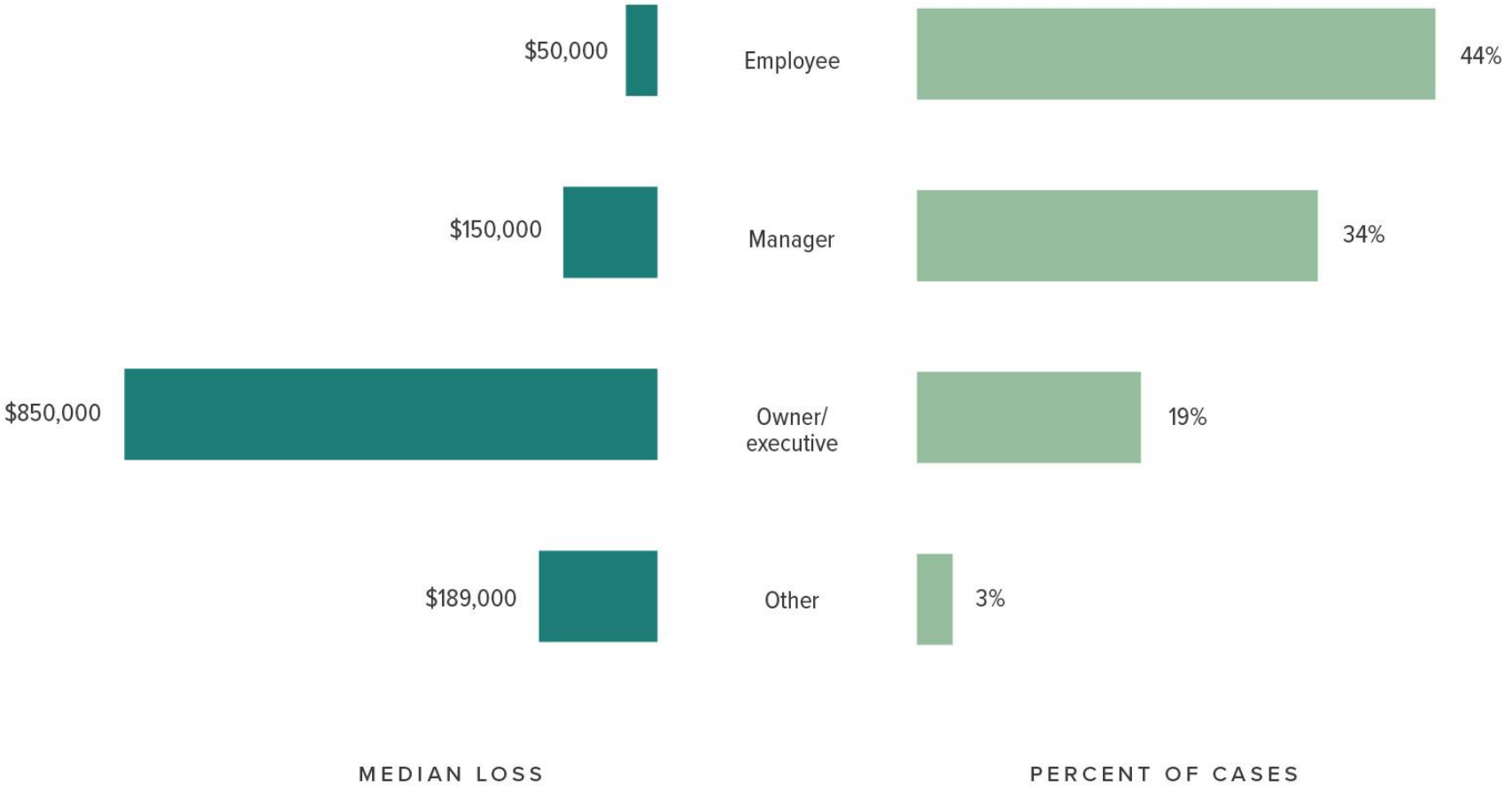
Vincent Walden
Compliance Innovator
vincentwalden1@gmail.com
+ 1 940 230 4648

Jay Sonbolian
Principal, EY
jay.sonbolian@ey.com
+ 1 617 407 0768

Appendix – examples

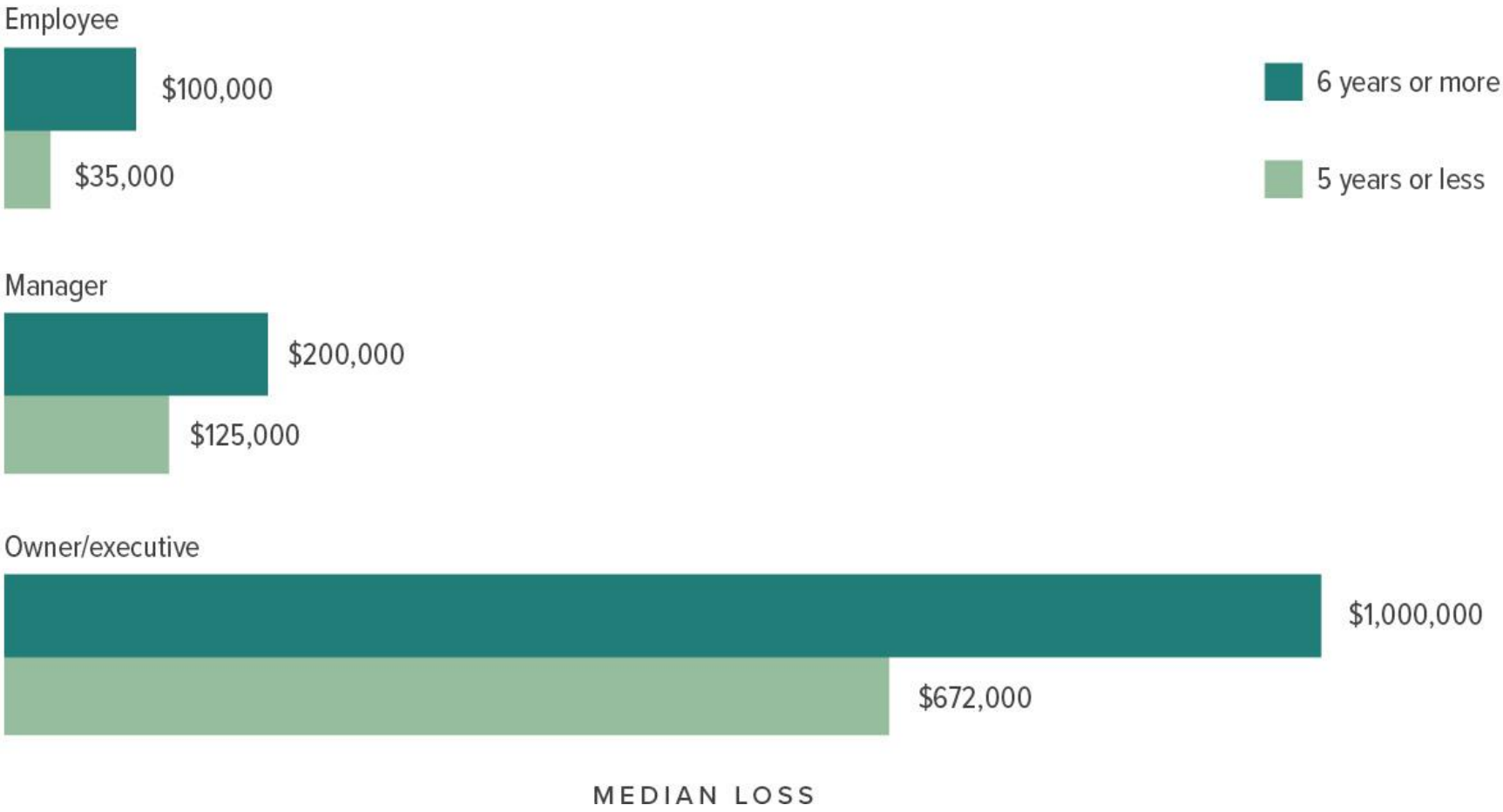
ACFE 2018 report to the nations

FIG. 24 **How does the perpetrator's level of authority relate to occupational fraud?**



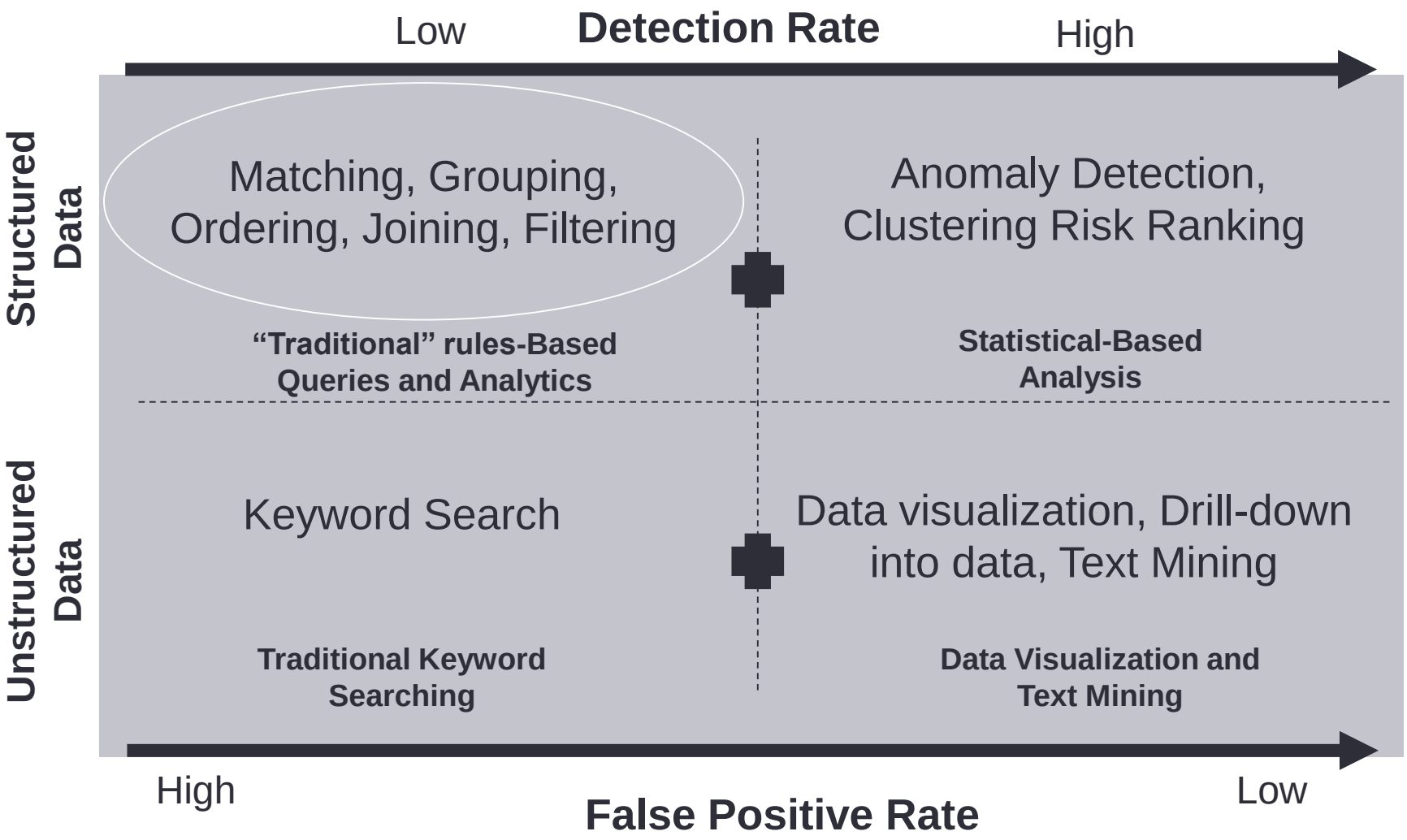
ACFE 2018 report to the nations

FIG. 27 **How does the perpetrator's tenure relate to median loss at different levels of authority?**



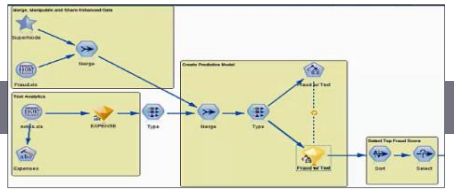
Forensic analytics maturity model

Beyond traditional “rules-based queries” – consider all four quadrants



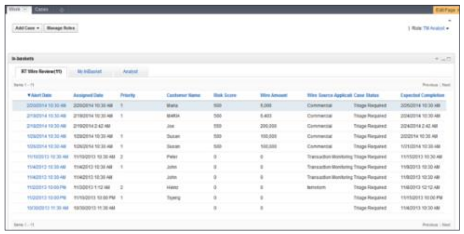
Elements of an effective monitoring program

Visualization and risk scoring to detect high risk vendors, customers or employees

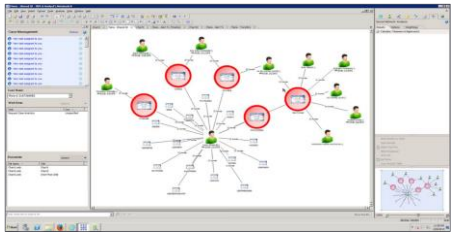


Statistical: Apply fraud insights and automated alerts to take action in real or near time – when it matters

Case Management: Assign tasks, flag transactions and train the predictive model



Pattern and Link: Uncover hidden relationships and conflicts of interest

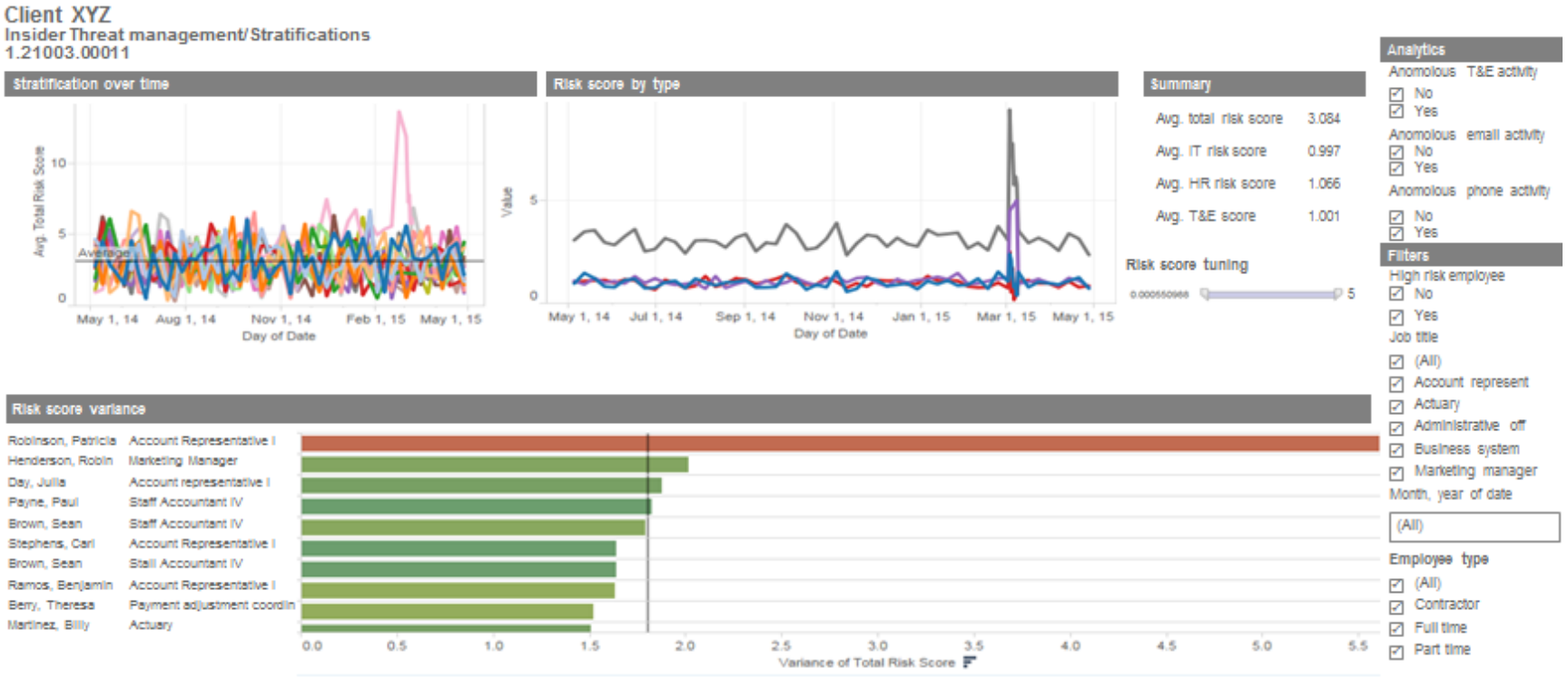


Insider threat “kill chain”
A proactive detection and disruption of insider activity

Insider Threat Attack (Kill) Chain Progression

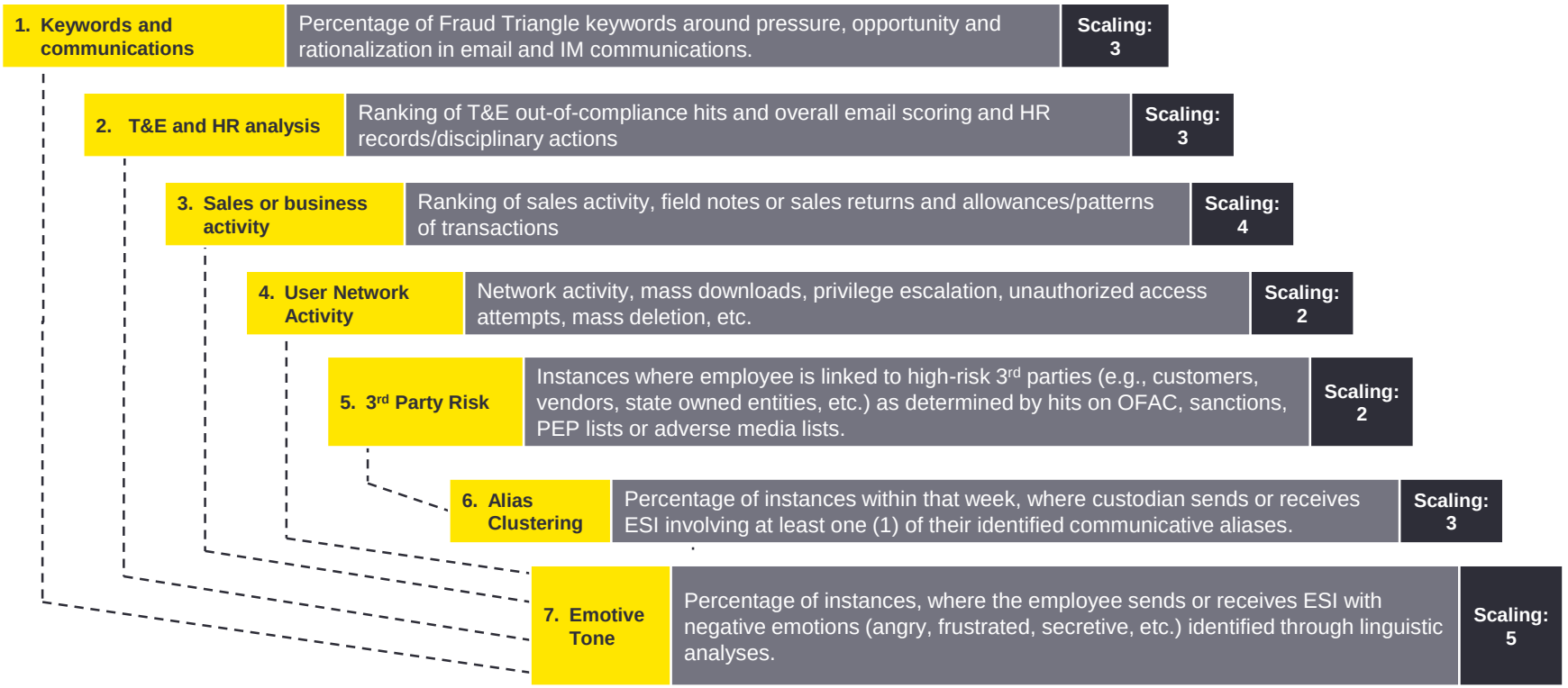
Recruitment/Tipping Point			
	Risk profile	**Vulnerability**	**Motivation**
	► Level of access ► Prior employment history ► Employee segmentation ► Compliance training record ► Criminal history ► HR record ► Personality ► Association with disgruntled former employee	► Drug or gambling habits ► Financial difficulties ► Mental health and wellbeing ► Relationship duplicitousness ► Mindset and psychology	► Performance history ► Termination or redundancy ► Under performance management ► Limited career progression ► Resignation or job searching ► Actively disengaged ► Overworked ► Overseas links and/or travel ► Contacts with competitors
Data sources	► HR systems ► CV and LinkedIn ► External checks ► Communications (content) ► Communications (pattern) ► Social media	► Communications (content) ► Communications (pattern) ► Payroll ► HR systems ► Whistleblower(s) ► Web history and social media ► Corporate card	► HR systems ► Web history and social media ► Communications (content) ► Communications (pattern) ► Phone logs ► Travel records ► Whistleblower(s)

Insider threat dashboard example



Layering example: Employee risk ranking

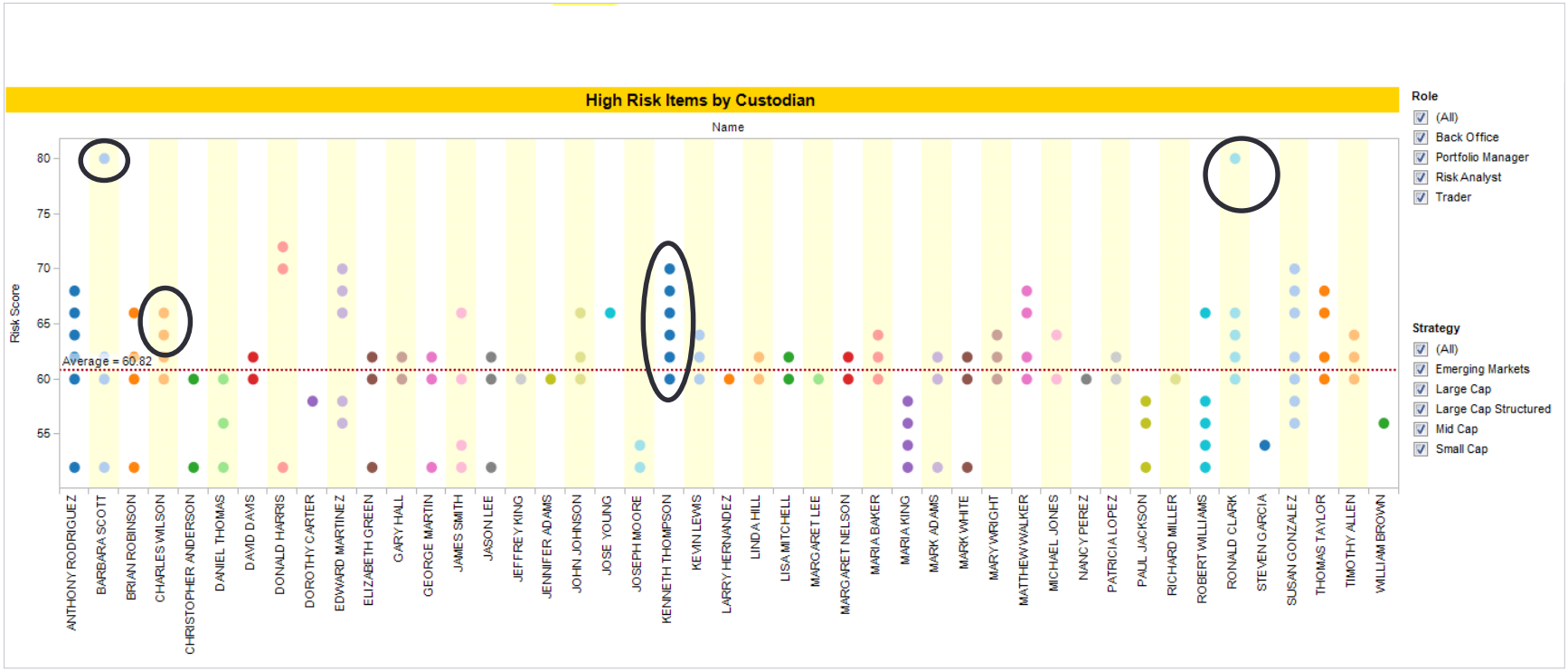
Scored by employee and time period based on multiple criteria and data sources



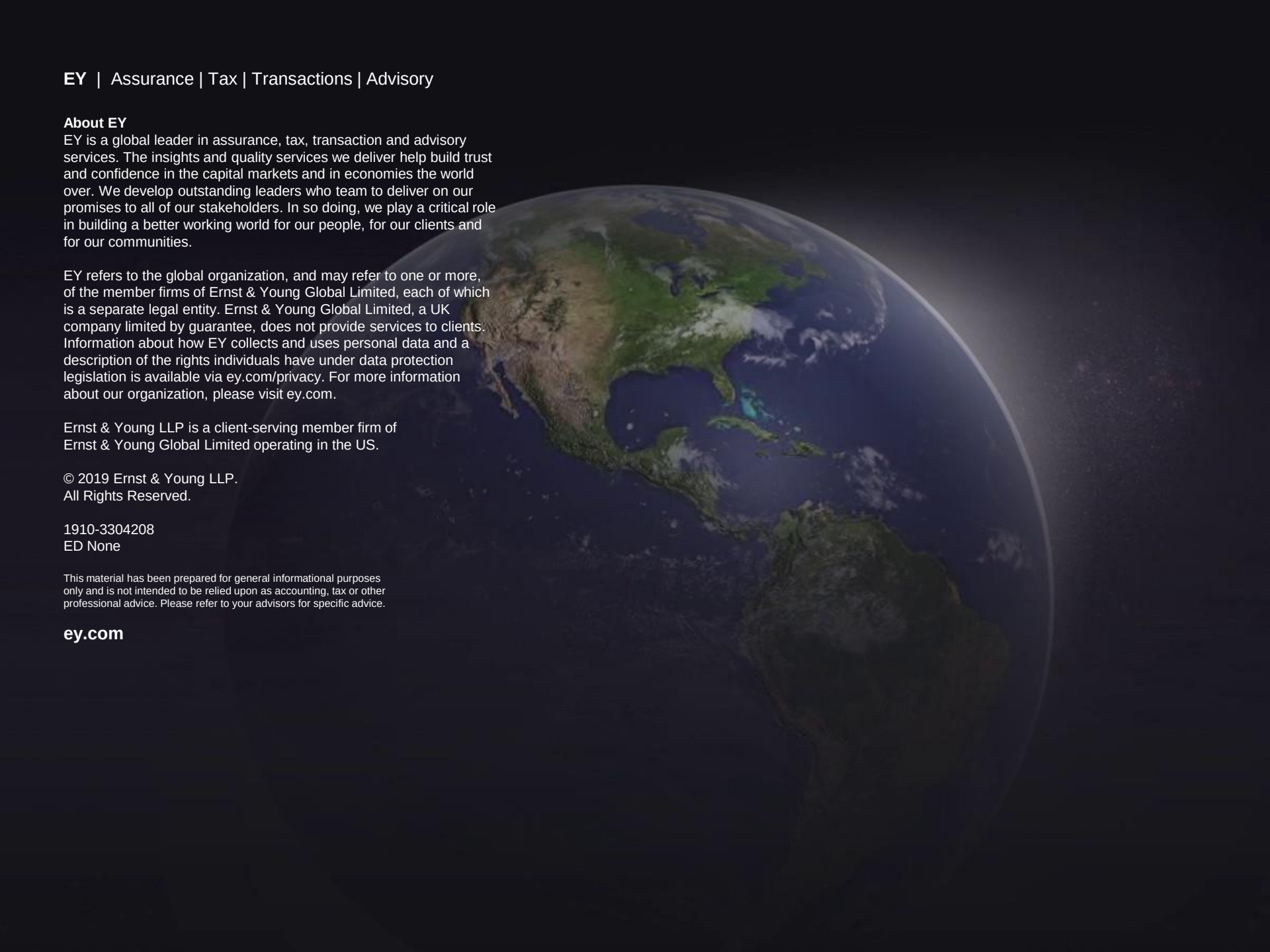
Custodian	C1	C2	C3	C4	C5	C6	C7	Scaling C1	Scaling C2	Scaling C3	Scaling C4	Scaling C5	Scaling C6	Scaling C7	Score
A, Week 1	1	3	3	4	6	2	3	3	3	4	2	2	3	5	**45**
A, Week 2	2	2	4	5	3	4	2								**37**

Employee risk ranking model

Risk Scoring Model – peer stratification dashboard review – email and transactions



Peer Stratification



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. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation is available via ey.com/privacy. 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.

1910-3304208
ED None

ey.com