# Identifying hidden risks using data analytics

Data analytics and AI webcast series

January 24, 2024

# Agenda

| | |
|---|---|
| 01 | Introduction |
| 02 | Risk-related analytics |
| 03 | Continuous risk assessment concepts |
| 04 | Advanced risk-related analytics |
| 05 | Technology considerations |
| 06 | Wrap-up and Q&A |

# Presenter

**Steve Biskie**

Principal, risk consulting
National SAP risk & automation services leader
Steve.Biskie@rsmus.com

- 25+ years data analytics for audit, compliance, and investigations
- Developed aci Learning’s Successful Audit Analytics Courses (formerly MIS Training Institute)
- Led strategy and audit analytics implementations in the Fortune 100 through the middle market
- Passionate about the value data mining can provide to identify, quantify, and monitor risk/fraud

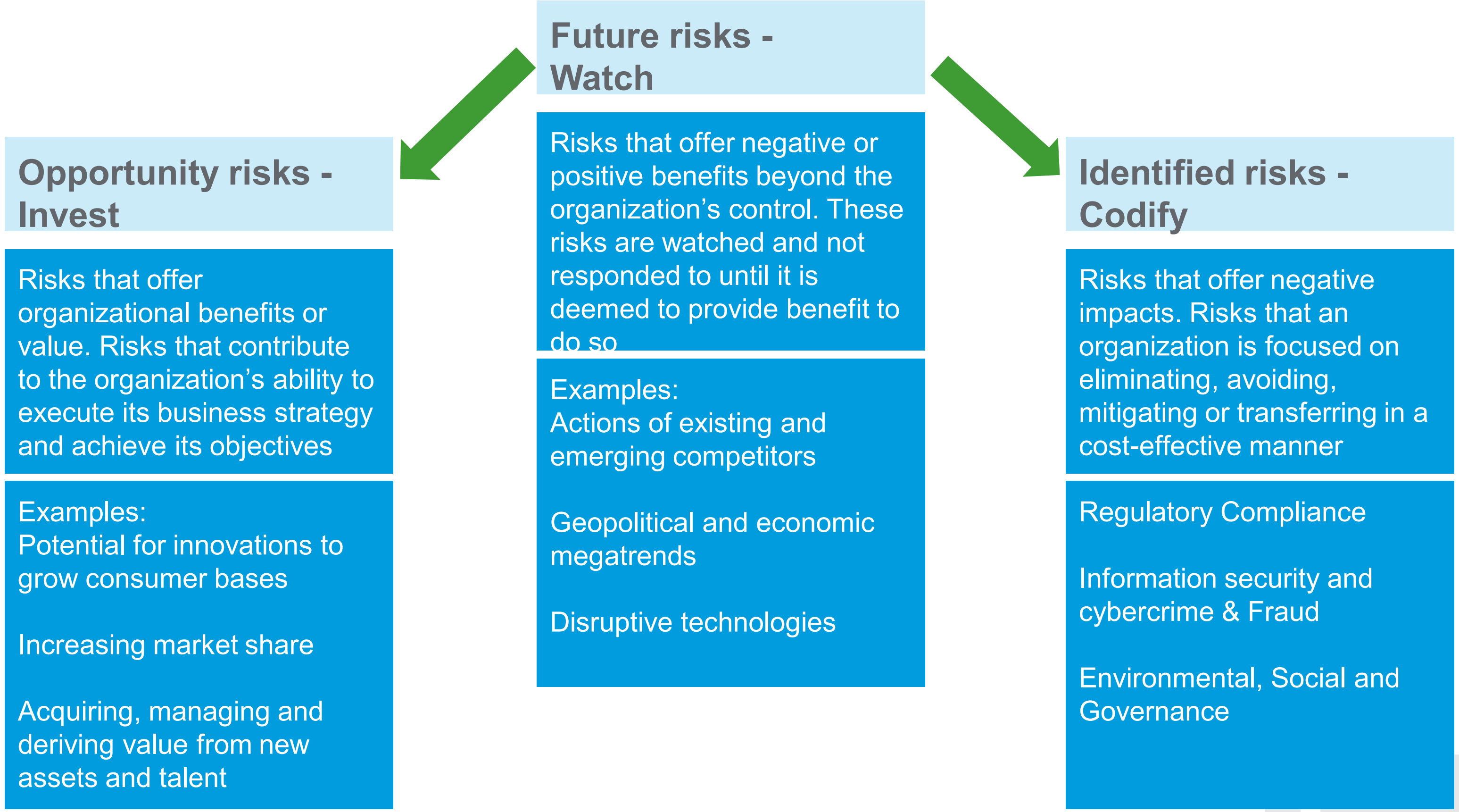
# Concept: risk categories

**Thinking differently**
Risks generally fall into three categories and the response to each will be different. To drive organizational value a shift in focus to opportunity risk is imperative.

How does your organization identify and respond to risk?

Do you have tangible information to help you understand timing and impact?

What are our unknown unknowns?



**Future risks - Watch**

Risks that offer negative or positive benefits beyond the organization's control. These risks are watched and not responded to until it is deemed to provide benefit to do so

Examples:
Actions of existing and emerging competitors

Geopolitical and economic megatrends

Disruptive technologies

**Opportunity risks - Invest**

Risks that offer organizational benefits or value. Risks that contribute to the organization's ability to execute its business strategy and achieve its objectives

Examples:
Potential for innovations to grow consumer bases

Increasing market share

Acquiring, managing and deriving value from new assets and talent

**Identified risks - Codify**

Risks that offer negative impacts. Risks that an organization is focused on eliminating, avoiding, mitigating or transferring in a cost-effective manner

Regulatory Compliance

Information security and cybercrime & Fraud

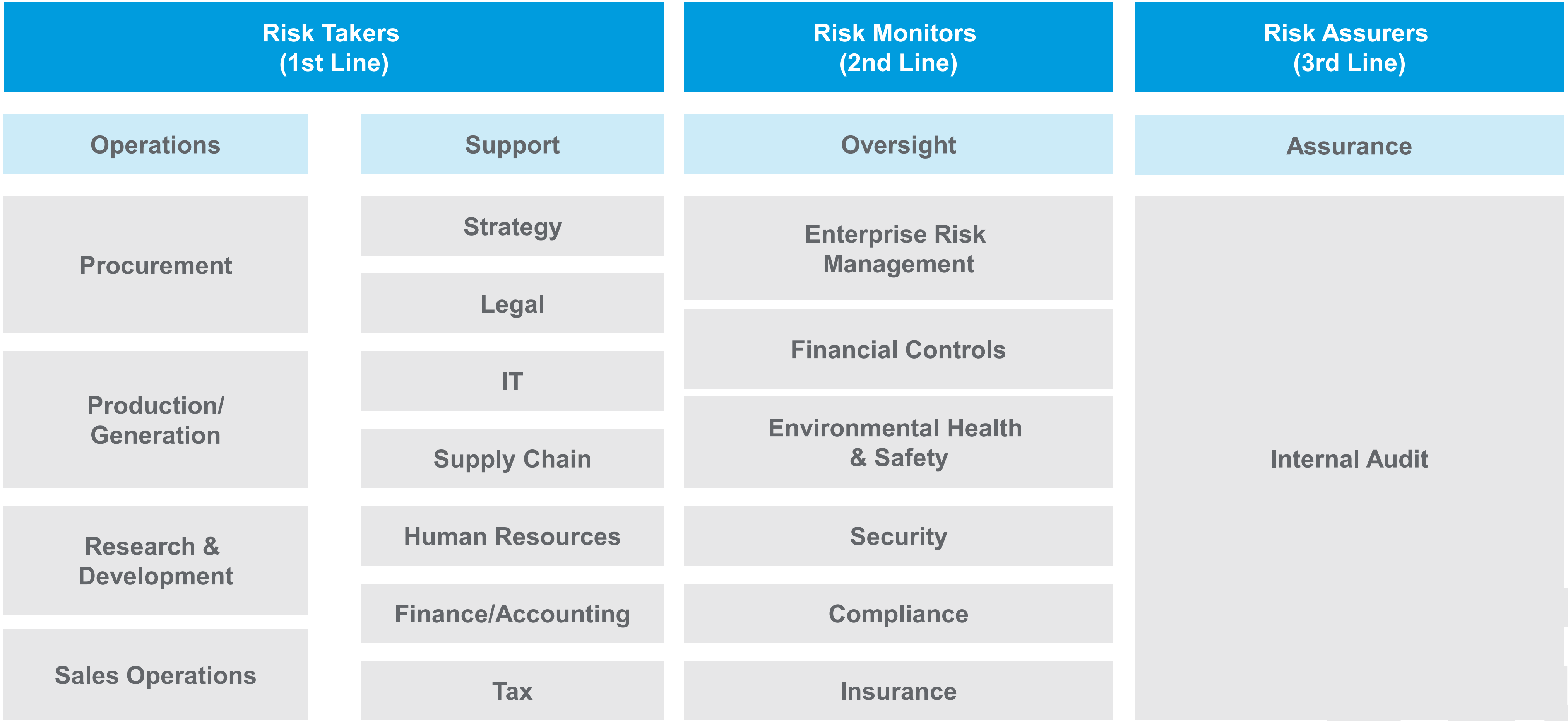
Environmental, Social and Governance

Organization that understand the above risk categories, have efficient and effective processes to **manage identified risks**, have **information and analysis on future risks** and **invest in opportunity risks** that will perform better over time.

# Concept: Three lines

## Institute of Internal Auditors

**Thinking differently**
Organizations drive value through risk management by identifying and responding to risk efficiently across all three lines of defense.



**Risk Takers (1st Line)**

Operations
- Procurement
- Production/ Generation
- Research & Development
- Sales Operations

Support
- Strategy
- Legal
- IT
- Supply Chain
- Human Resources
- Finance/Accounting
- Tax

**Risk Monitors (2nd Line)**

Oversight
- Enterprise Risk Management
- Financial Controls
- Environmental Health & Safety
- Security
- Compliance
- Insurance

**Risk Assurers (3rd Line)**

Assurance
- Internal Audit

# Risk-related analytics

# Risk-related analytics generally fall into four main categories

## LEARN

- Assess data quality
- Profile business activity
- Define normal (or wrong)
- Model process outcomes and residual risks
- Catalog key risk / controls
- Review org, process, and system changes
- Review 1st / 2nd line KRIs
- Exploratory Data Analysis

## CATCH

- Identify new or persistent risks
- Gaps between system configuration and transaction processing
- Detect anomalous / irregular patterns
- Identify noncompliance
- Detect fraudulent activity
- Detect abuse of company resources
- Flag waste and abuse

## CONFIRM

- Attest to the effectiveness of a control
- Verify existence of an asset or an action
- Calculation is materially accurate / correct
- Performance of a model or process is "in bounds"
- Provide effective challenge
- Corroborate an allegation
- Substantiate an audit finding

## VALUATE

- Assess an event's impact
- Estimate likelihood or probability
- Calculate level of effort, return on investment, or cost of implementation
- Calculate the total cost of a control
- Assess the impact of process improvements
- Estimate reserve amounts

Each mode can be ad hoc, repeatable or continuous

# Example library of risk-related analytics

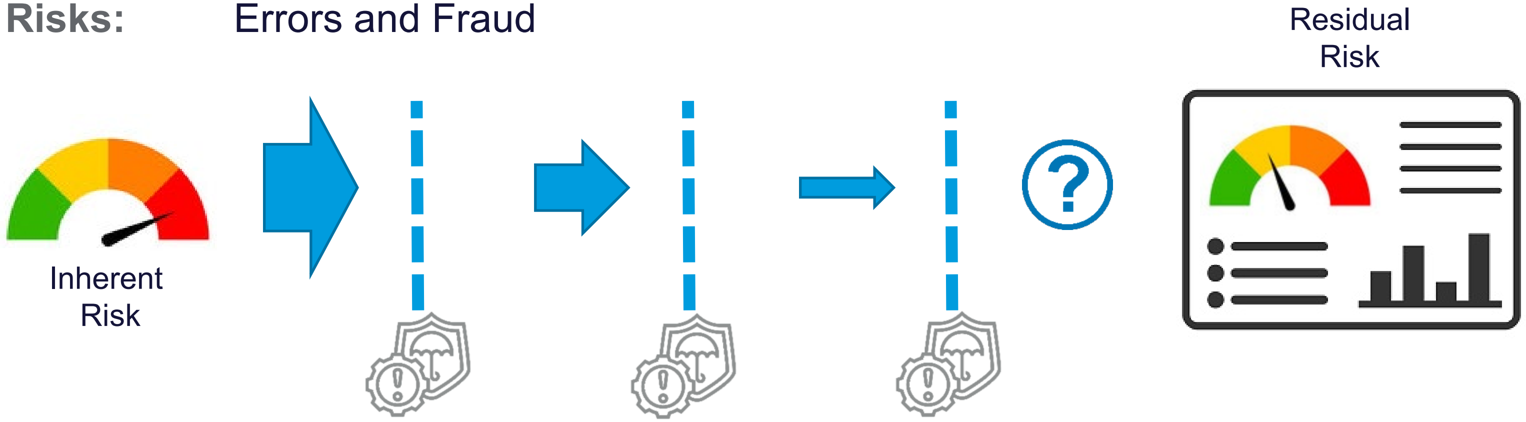
| | TE/PCARD | P2P | R2R | F2S | H2R | IT/ITGC |
|---|---|---|---|---|---|---|
| **Ad hoc** | • Spender / Merchant profiling<br>• Spend near home location<br>• Approval pattern analysis<br>• Cardholder not active employee<br>• Match to bank feeds<br>• Rebate optimization | • One time vendor use<br>• Bid rigging<br>• Out of sequence activity<br>• Open credit memo<br>• Redirected payments<br>• Disbursements not through AP<br>• Time value of money | • Profiling JEs by poster, approver, day, time, size, location<br>• JE approvals within authorization limits<br>• Fixed asset depreciation recalculation<br>• Ratio analysis | • MRP purchase item, but in inventory<br>• Inventory as percent of sales<br>• Material Master review | • Skills gaps<br>• Health & Safety incidents<br>• Healthcare claims<br>• Suspicious pay changes<br>• Unsupported time entries<br>• Per diem abuse | • Logical/physical access<br>• Incident profiling<br>• Application changes<br>• SLA verification<br>• Software licensing<br>• Patch compliance |
| **Repeatable** | • Meals and attendees<br>• Unassigned corporate card transactions<br>• Unusual lodging and airfare<br>• Excessive meals and entertainment<br>• Charges to miscellaneous expense categories | • PO changes over time<br>• 3-way match<br>• Sole source hi-risk vendors<br>• Concentrated transaction<br>• Tolerance abuse<br>• Posting to risky GL<br>• Changes to high-risk vendor master fields | • Aged CIP<br>• Assets in use beyond expected life<br>• Unusual account posting combinations<br>• Posting to period not near entry date<br>• Manual posting to system account | • Aged finished goods<br>• Aged WIP<br>• Vendor managed inventory<br>• Unusual movements to obsolete/scrap<br>• Excessive returns | • Suspicious work times<br>• Off cycle payments<br>• Excessive Overtime<br>• Missing training records<br>• Ghost employees<br>• Negative PTO balances<br>• Unauthorized HR changes | • Backup log review<br>• Event log review<br>• Active Directory attribution testing<br>• Account provisioning<br>• Termination testing<br>• Patch monitoring<br>• Anti-X monitoring |
| **Optimized** | • Appropriate approval<br>• Unusual expense combinations<br>• Unauthorized merchant/MCC<br>• Outlier expenses and spenders<br>• Late Expenses / Past Due<br>• Abnormal timing between processes | • Unusual address<br>• Payment out of country bank<br>• Discounts not taken<br>• Reanimated / evergreen PO<br>• Invoice number formats<br>• Predated / Backdates invoices<br>• Invoices with no PO | • Non-standard JE's, including unusual reversals and adjustments<br>• Segments created/changed<br>• Entries to seldom-used/dormant accounts<br>• Entry by unexpected user ID | • Time in Quality Inspection<br>• Timely inventory/cycle counts<br>• Floor-to-Sheet and Sheet-to-Floor sampling | **Utility Analytics (Cross-Audit and Process)**<br>•Duplicate/split transaction<br>•Keyword search<br>•Transactional SoD<br>•Related parties<br>•Outlier/extreme values<br>•Suspicious times and dates | |

# Monitoring residual risk

Internal controls are intended to reduce risk but are generally not perfect.
What if you had visibility into the residual risk after your processes passed through your internal control procedures?

**Process:** Payroll

**Risks:** Errors and Fraud



- Wrong payee
- Early/late payment
- Over/under payment
- Wrong destination (address/bank)

If these indicators reveal low residual risk, how might this effect your audit approach?

**Internal controls**

- Restricted access
- Staff Training
- Segregation of Duties
- Rate change limits
- Systematic approvals
- Expense monitoring
- Bank account verification

# Leveraging data in a GRC platform

## DATA GATHERING

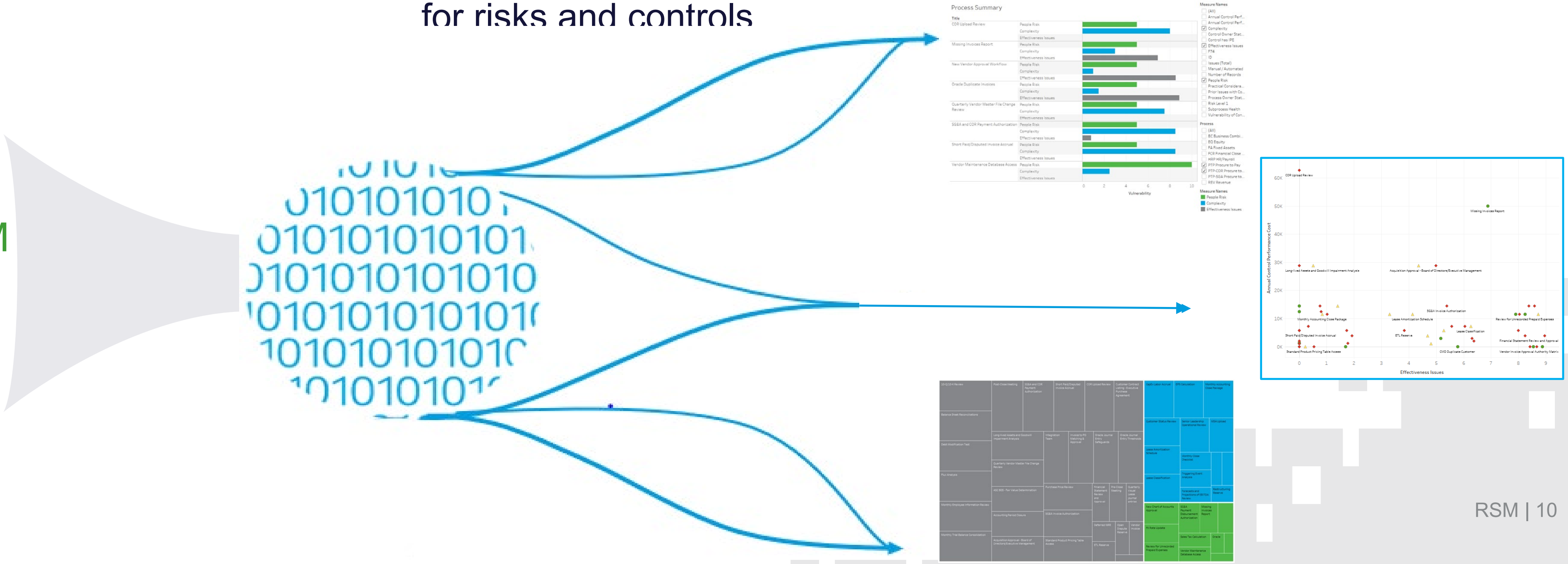
Data recorded throughout the GRC/SOX risk & control testing process holds information that can be transformed into valuable insights

## TRANSFORMATION & ANALYSIS

Extracted data is cleansed, transformed and analyzed to show YoY trends, key performance indicators and root cause details for risks and controls

## RISK INSIGHTS REPORTING

Dashboard visualizations provide an executive summary view of enhanced risk and control insights

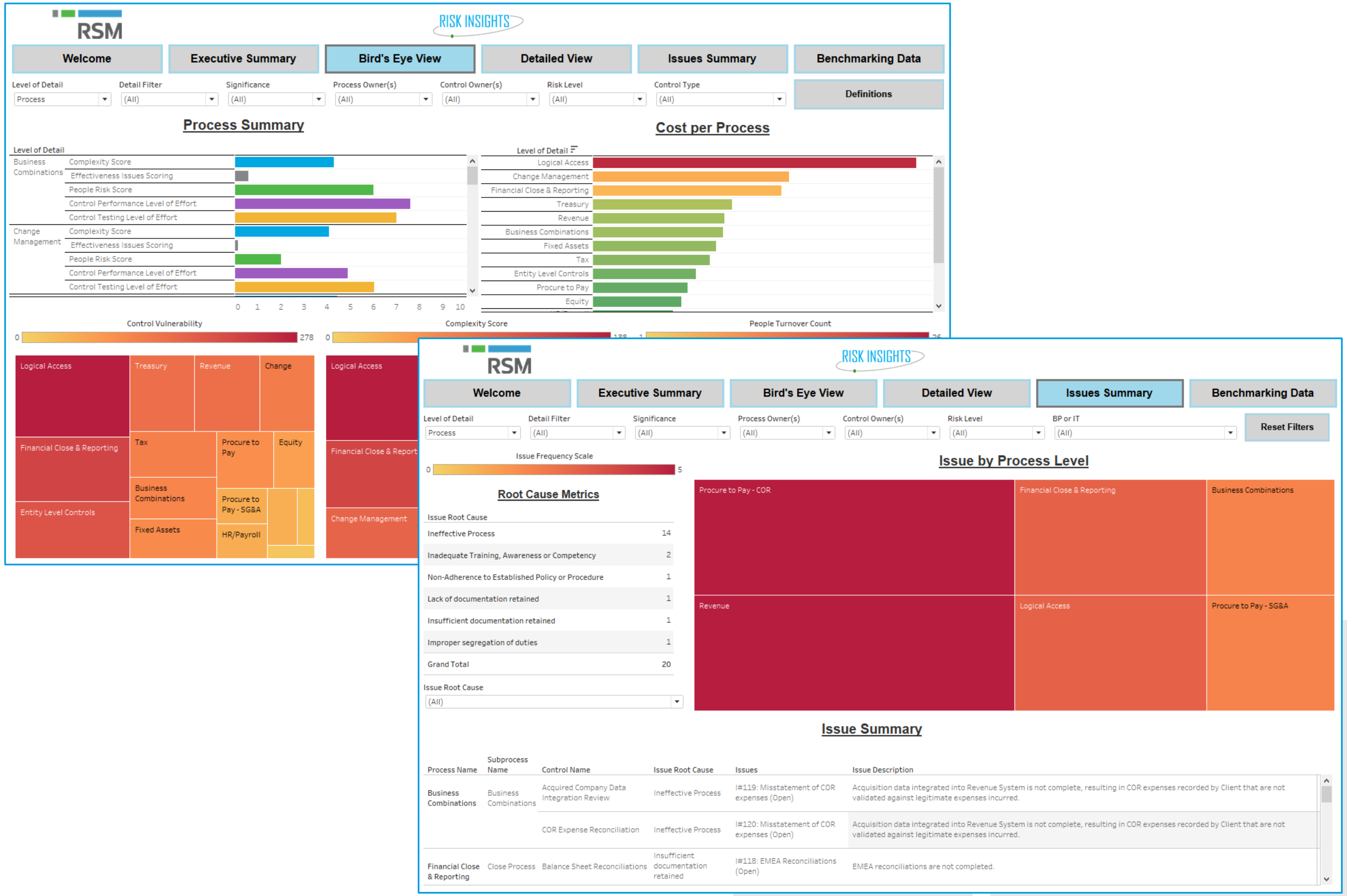


DATA FROM YOUR GRC PLATFORM

# What can we learn?

Facilitates meaningful discussion around control environment optimization:

- How can complex controls be automated?
- What are the most vulnerable process areas?
- What areas have the most turnover or dependency on an individual?
- Why did controls fail this year?
- Which controls are the most costly?



Root Cause Metrics

| Issue Root Cause | |
|---|---|
| Ineffective Process | 14 |
| Inadequate Training, Awareness or Competency | 2 |
| Non-Adherence to Established Policy or Procedure | 1 |
| Lack of documentation retained | 1 |
| Insufficient documentation retained | 1 |
| Improper segregation of duties | 1 |
| Grand Total | 20 |

Issue Root Cause: (All)

Issue Summary

| Process Name | Subprocess Name | Control Name | Issue Root Cause | Issues | Issue Description |
|---|---|---|---|---|---|
| Business Combinations | Business Combinations | Acquired Company Data Integration Review | Ineffective Process | I#119: Misstatement of COR expenses (Open) | Acquisition data integrated into Revenue System is not complete, resulting in COR expenses recorded by Client that are not validated against legitimate expenses incurred. |
| | | COR Expense Reconciliation | Ineffective Process | I#120: Misstatement of COR expenses (Open) | Acquisition data integrated into Revenue System is not complete, resulting in COR expenses recorded by Client that are not validated against legitimate expenses incurred. |
| Financial Close & Reporting | Close Process | Balance Sheet Reconciliations | Insufficient documentation retained | I#118: EMEA Reconciliations (Open) | EMEA reconciliations are not completed. |

# Continuous risk assessment concepts

# What’s the difference?

## Continuous monitoring:

**Purpose**: To ensure that business processes and controls are working as intended and to identify any anomalies or deviations from expected performance.

**Focus**: Mainly concerned with the operational aspects ofWhat’s the difference? an organization, such as compliance with procedures, efficiency of operations, and reliability of financial reporting.

## Continuous risk assessment:

**Purpose**: To anticipate and respond to changes in the organization's internal and external environments that might impact its ability to achieve its objectives.

**Focus**: More strategic and forward-looking. Considers a variety of factors that could pose risks to the organization, including changes in market conditions, regulatory environments, technological advancements, and internal process changes.

In summary, continuous monitoring is more about ensuring current processes and controls are functioning correctly, while continuous risk assessment is about understanding and responding to current and potential future risks

# Example risk indicators

## Internal:

Spike in high-priority IT tickets open > 3 days for an application that has been historically stable

% turnover within management in a division differs from other divisions

Increase in customer complaints using words and phrases like “late” or “wrong product”

A control owner for several key SOX controls had a recent had a significant HR change (e.g., change in department or departure form organization)

## External:

Sudden and significant increase in negative sentiment for a key business partner (based on news & social media comments)

Proposed new legislation affecting a key market segment gaining traction based on automated news analysis

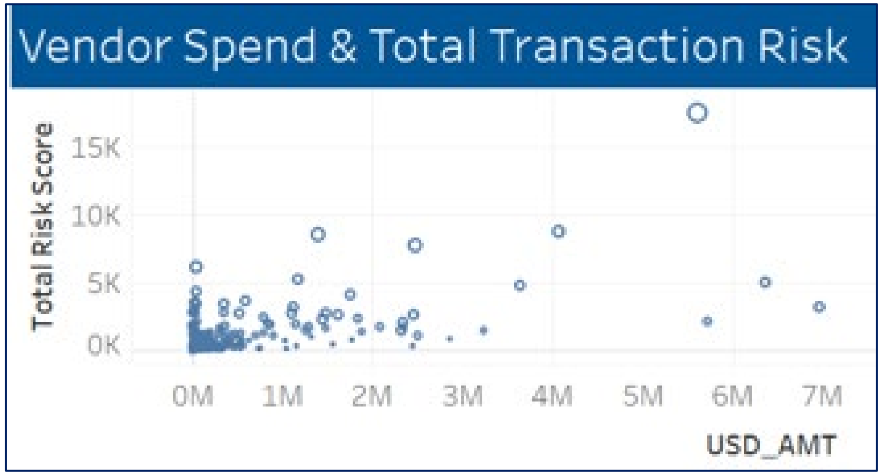
The D&B credit rating of a sole-source vendor drops significantly

# Key to successful continuous risk assessment: risk scoring

As you mature your data-driven risk assessment, you may ultimately find ourself monitoring hundreds of KRIs to identify items for investigation. Aggregating risk scores (by location, division, manager, customer, etc.) can help focus efforts in the riskiest areas.

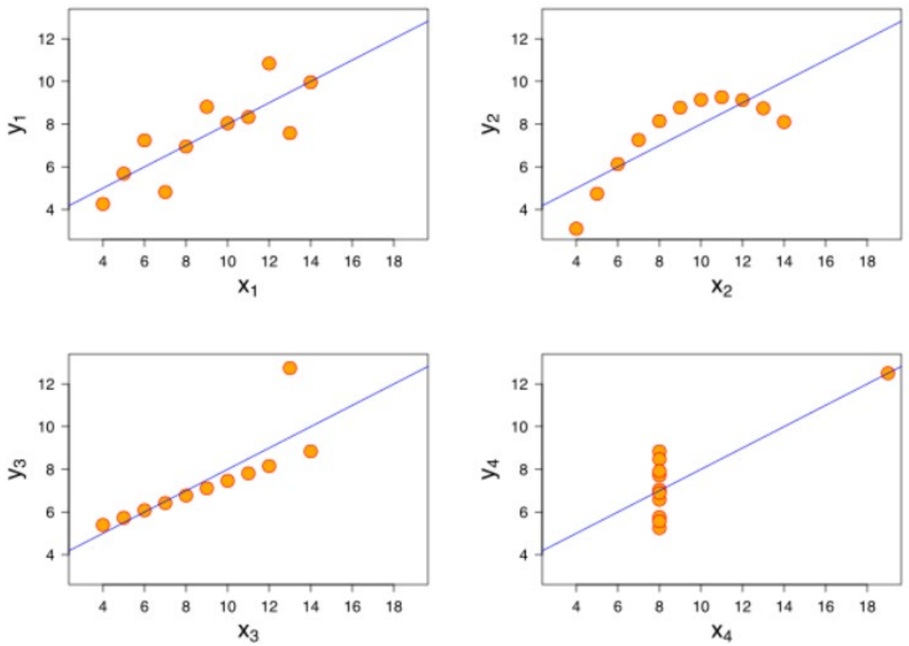
Combining:

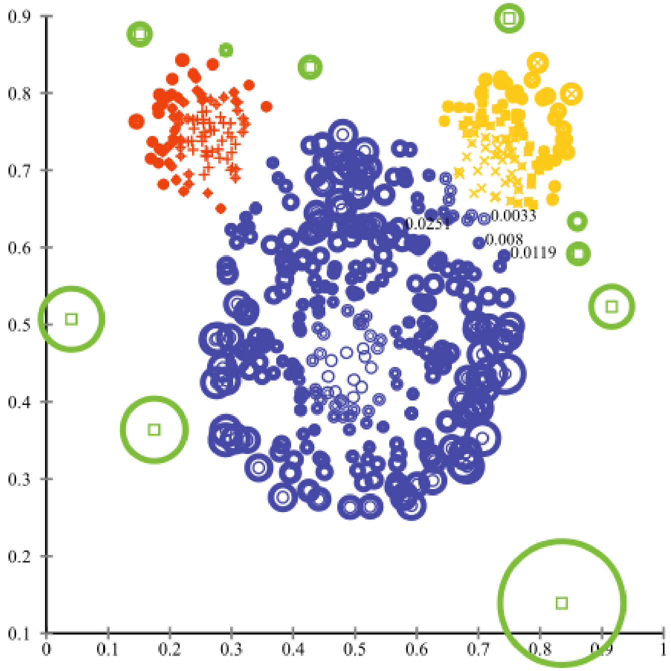
- **Rule based analytics** such as round payments, missing fields, duplicate transactions, etc.
- **Statistical analytics** such as unusual debit/credit account combinations, abnormally high amounts for given budget line item, etc.
- **External data** such as third-party due diligence screening information.
- **Machine learning** to tailor scoring based on historical investigations.



# Advanced risk-related analytics

# Advanced algorithms: anomaly detection using clustering





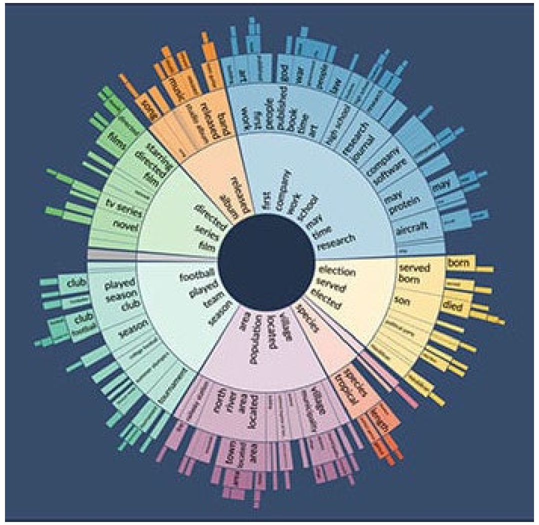
Calculating an average is so 1990s (Anscombe’s quartet)

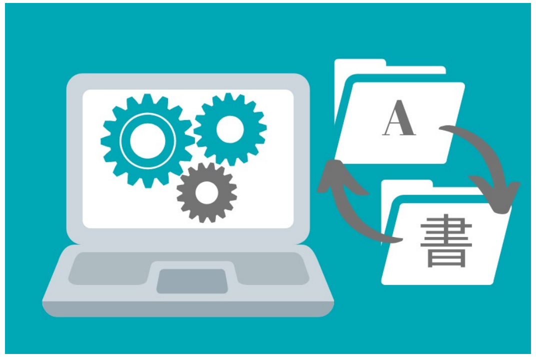
Clustering is a better way of anomaly detection

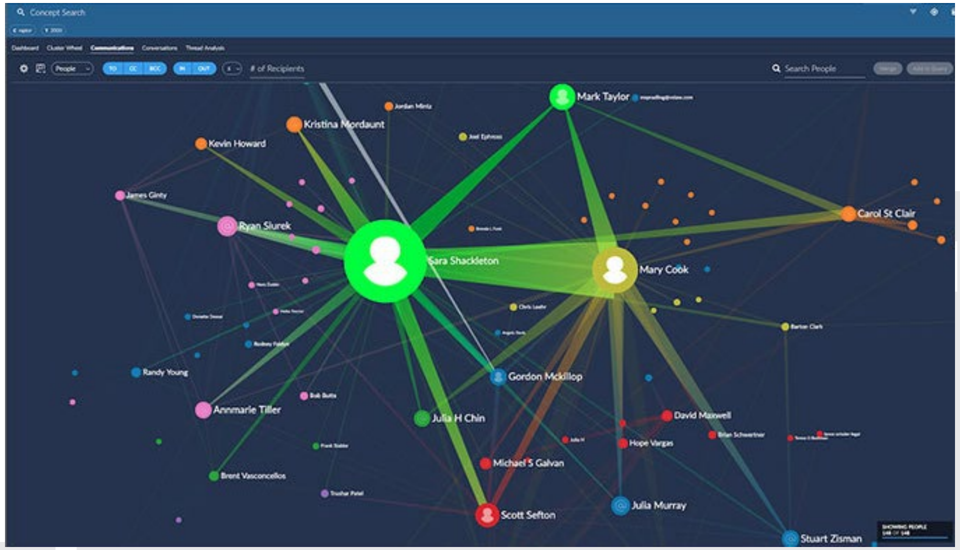
# AI improves email, chat and document review for risk identification

AI goes beyond traditional keyword searching:

- Sentiment analysis
- Communication network diagrams
- Conceptual grouping of topics
- Automated transcription of voice messages / videos
- Automated translation
- Computer vision

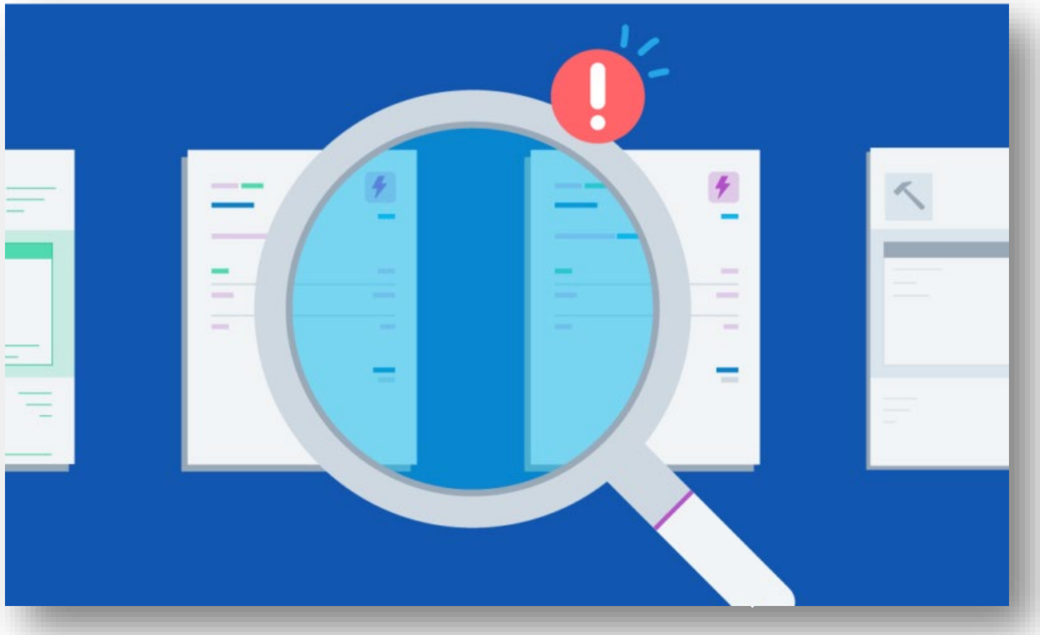


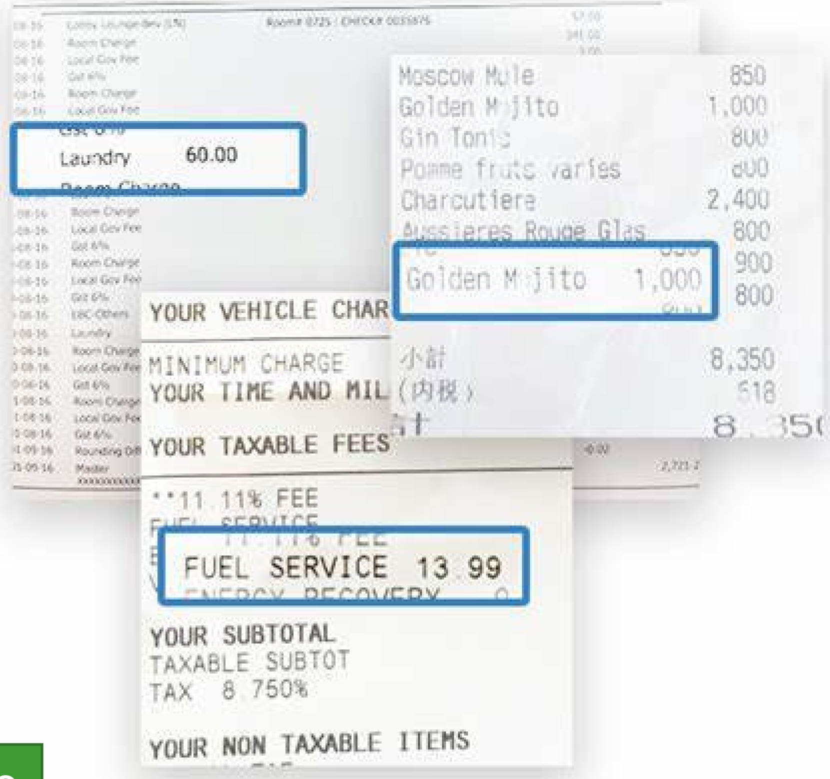




# Computer vision for compliance violations and fraud detection

Integrating technology with AI and computer vision in an organization's T&E process can help detect issues that would often be missed, such as reimbursement for duplicative invoices or unauthorized line items.





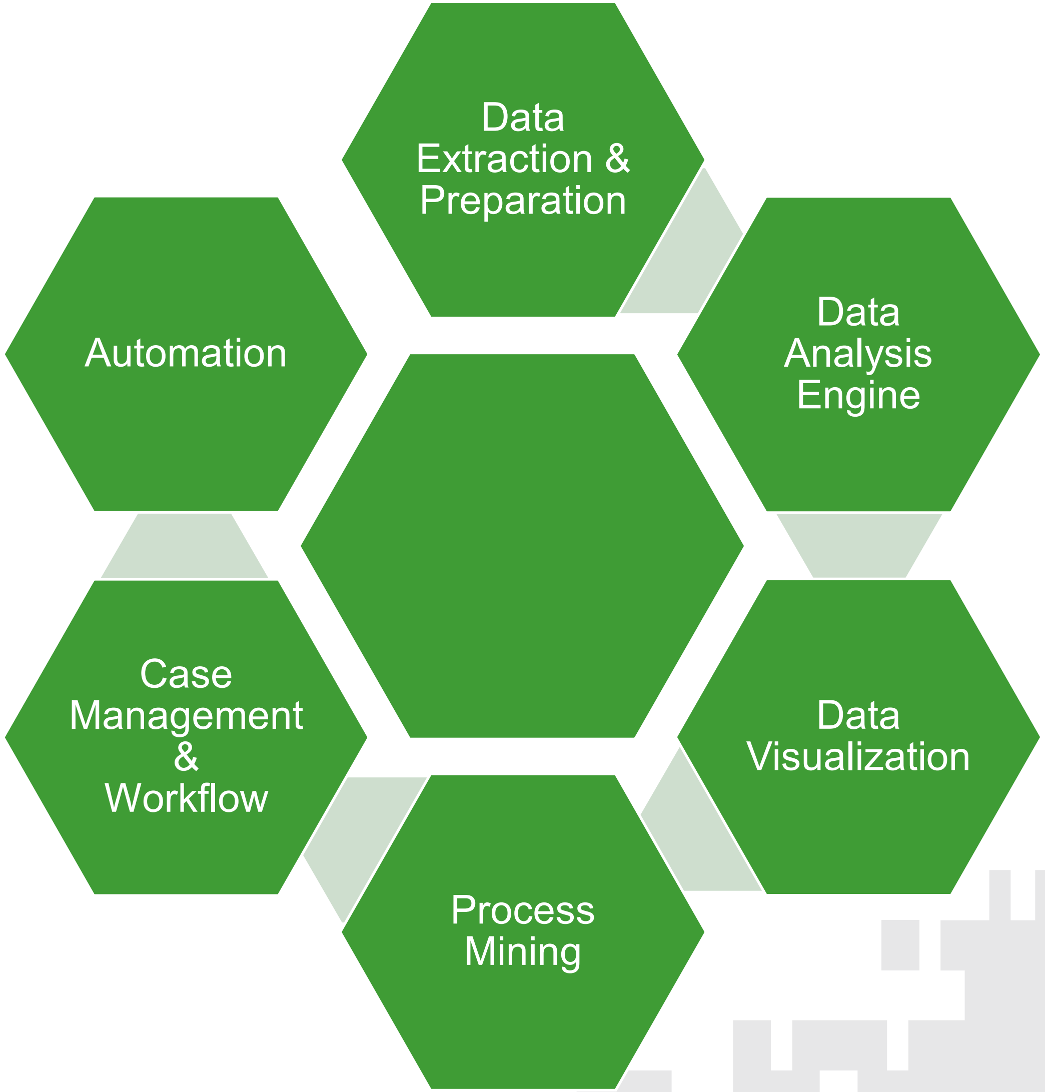
In more advanced use cases, AI and ML could even compare receipt amounts to prices listed on a menu or website

# Technology considerations

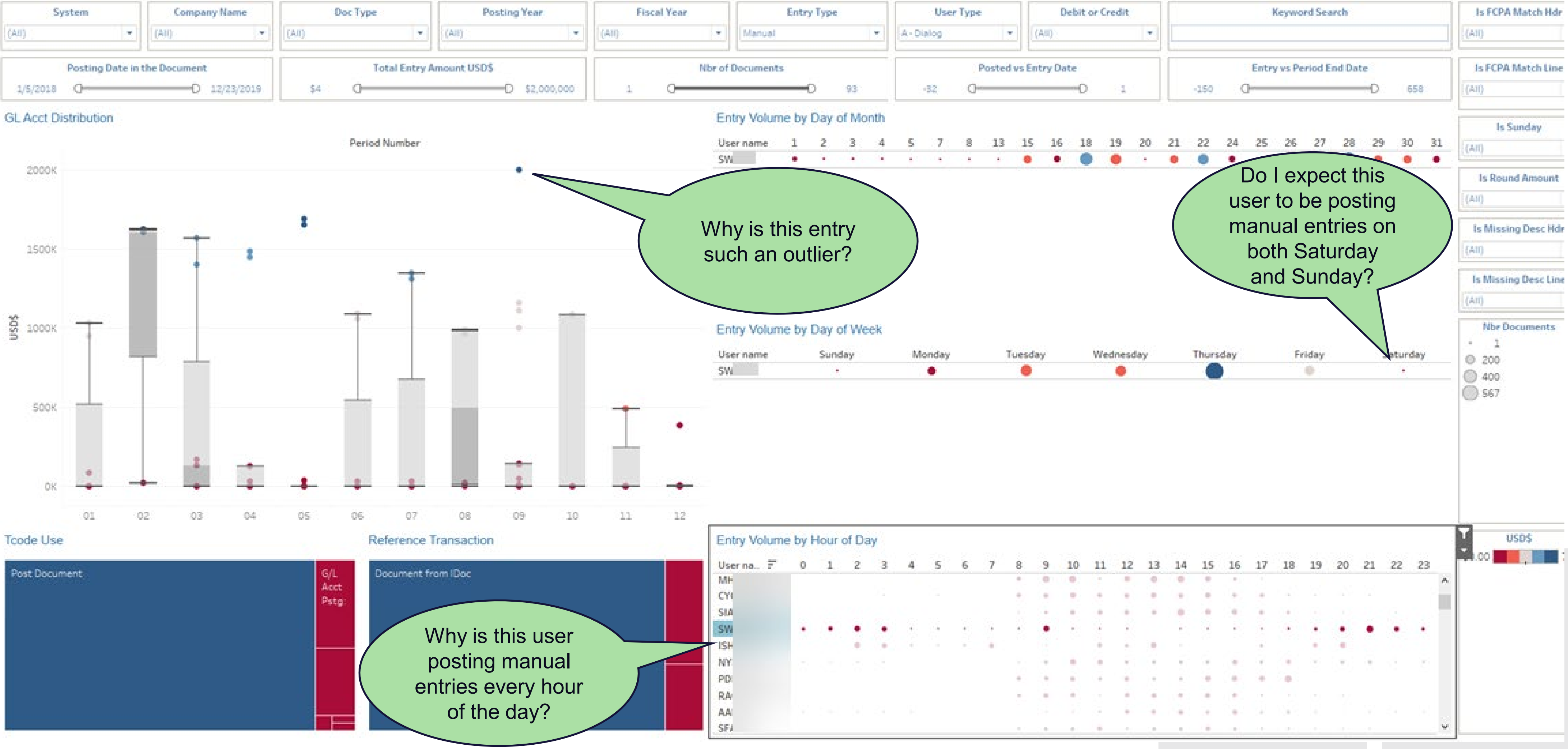
# The risk analytics toolbox

Like a “normal” toolbox:

- Each category of tool serves a different purpose
- Inexpensive tools may get you started, but there’s usually a reason some tools cost more than others
- The tools you need depend on what you’re trying to accomplish
  - But for those of you who are frugal-minded, just because you “can” pound a nail with the back of a screwdriver doesn’t mean you “should”



# Data visualization can help spot risks



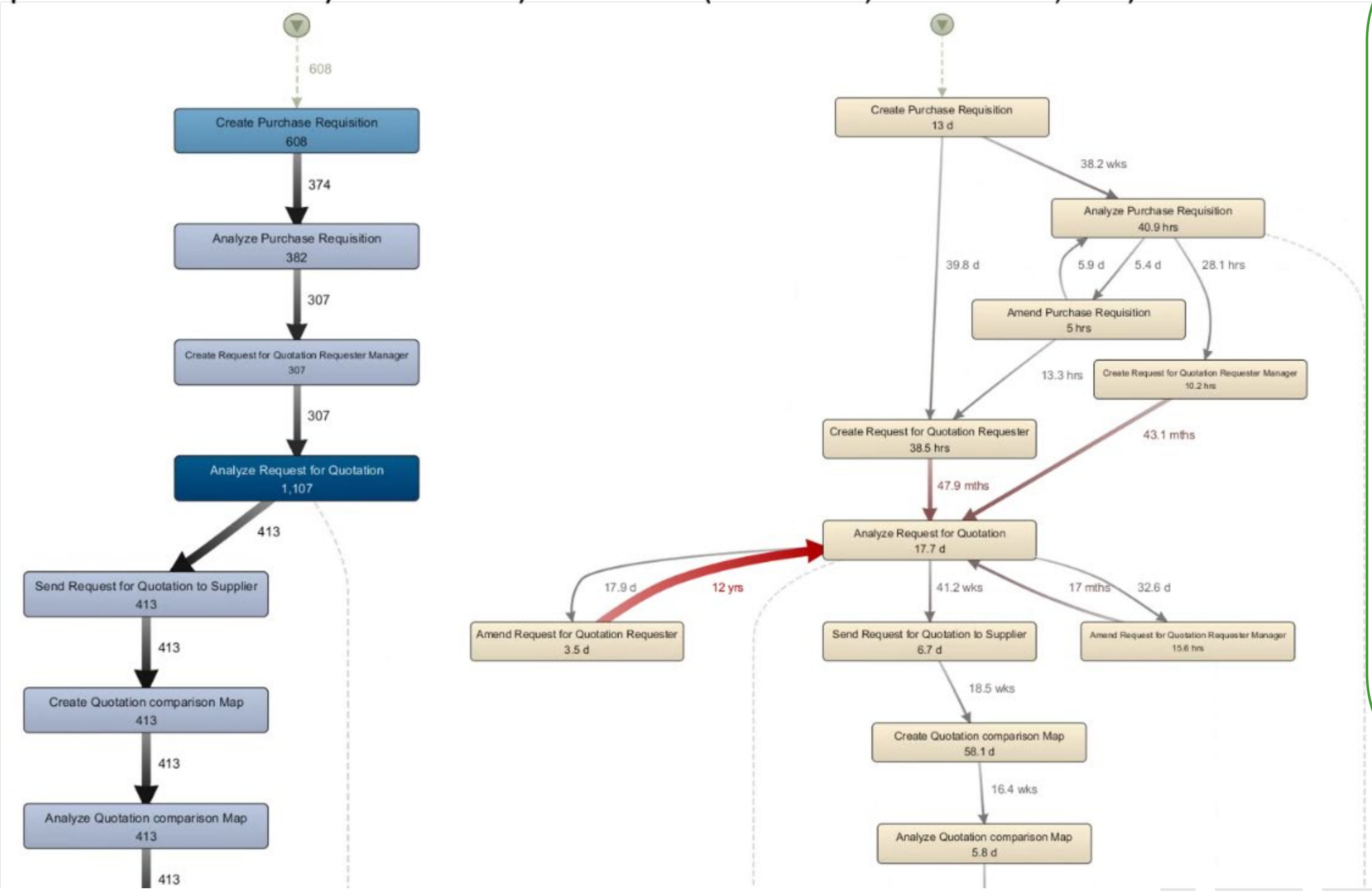
System: (All)
Company Name: (All)
Doc Type: (All)
Posting Year: (All)
Fiscal Year: (All)
Entry Type: Manual
User Type: A - Dialog
Debit or Credit: (All)
Keyword Search:
Is FCPA Match Hdr: (All)
Posting Date in the Document: 1/5/2018 – 12/23/2019
Total Entry Amount USD$: $4 – $2,000,000
Nbr of Documents: 1 – 93
Posted vs Entry Date: -32 – 1
Entry vs Period End Date: -150 – 658
Is FCPA Match Line: (All)
Is Sunday: (All)
Is Round Amount: (All)
Is Missing Desc Hdr: (All)
Is Missing Desc Line: (All)

Why is this entry such an outlier?

Do I expect this user to be posting manual entries on both Saturday and Sunday?

Why is this user posting manual entries every hour of the day?

# Process mining helps visualize risk specific to the process flow



**Ideal process**
(what process owner usually has in mind)

**Real process**
(deviations, bottlenecks, etc.)

608
Create Purchase Requisition
608
374
Analyze Purchase Requisition
382
307
Create Request for Quotation Requester Manager
307
307
Analyze Request for Quotation
1,107
413
Send Request for Quotation to Supplier
413
413
Create Quotation comparison Map
413
413
Analyze Quotation comparison Map
413
413
Create Purchase Requisition
13 d
38.2 wks
Analyze Purchase Requisition
40.9 hrs
39.8 d
5.9 d
5.4 d
28.1 hrs
Amend Purchase Requisition
5 hrs
13.3 hrs
Create Request for Quotation Requester Manager
10.2 hrs
Create Request for Quotation Requester
38.5 hrs
43.1 mths
47.9 mths
Analyze Request for Quotation
17.7 d
17.9 d
12 yrs
41.2 wks
17 mths
32.6 d
Amend Request for Quotation Requester
3.5 d
Send Request for Quotation to Supplier
6.7 d
Amend Request for Quotation Requester Manager
15.6 hrs
18.5 wks
Create Quotation comparison Map
58.1 d
16.4 wks
Analyze Quotation comparison Map
5.8 d

Event logs containing an event ID, timedate stamp, user ID/role can reveal the true nature of a business process

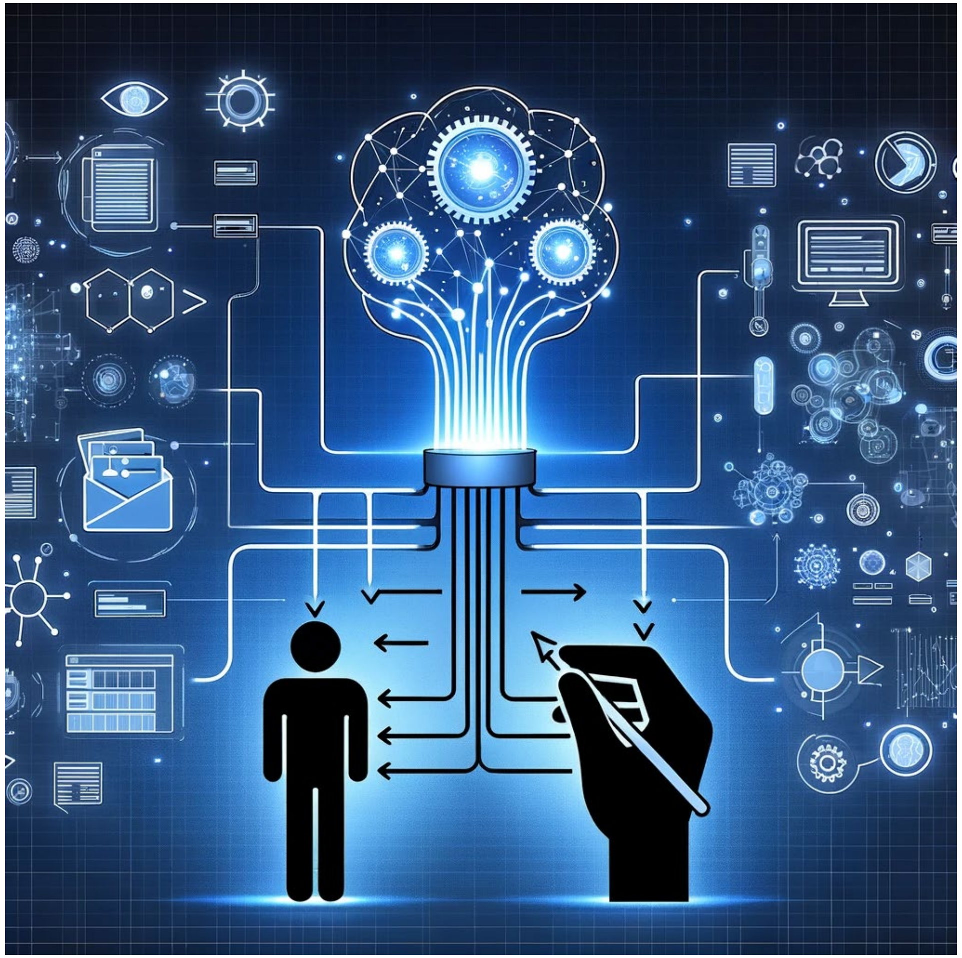
Process mining may show that actual process activity does not align with management's impression of how they think the process works

**Discover Hidden or Emerging Risks**

What process deviations don't we know about?

Is the process changing or getting more complex over time?

# Case management and workflow set the foundation for AI

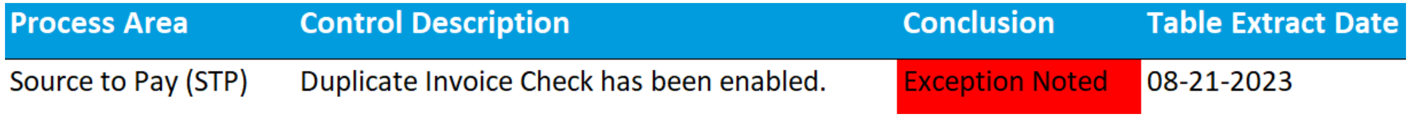


By routing suspected transactions/risks to the right people for analysis, you:

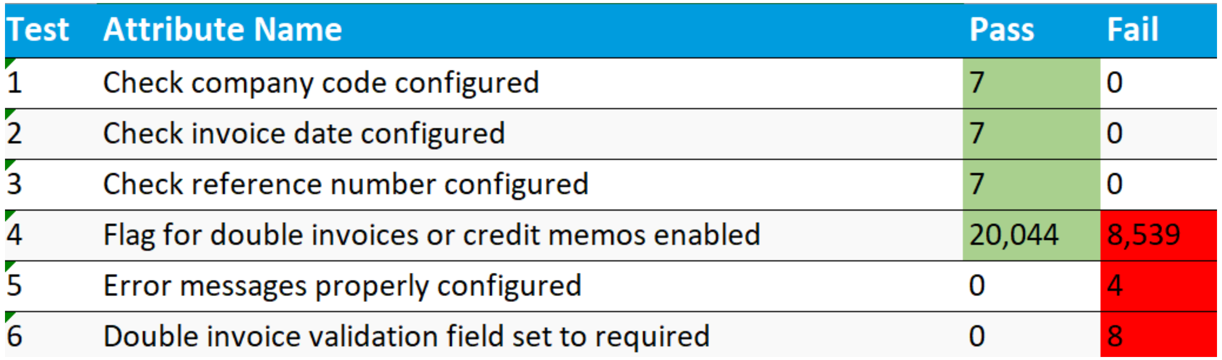
- Set the stage for taking action on risks closer to real-time
- Begin to differentiate between expected and unexpected risks
- Create a history of “tagged” cases

This data can now be used to feed machine learning algorithms to further improve your risk identification, quantification, and monitoring

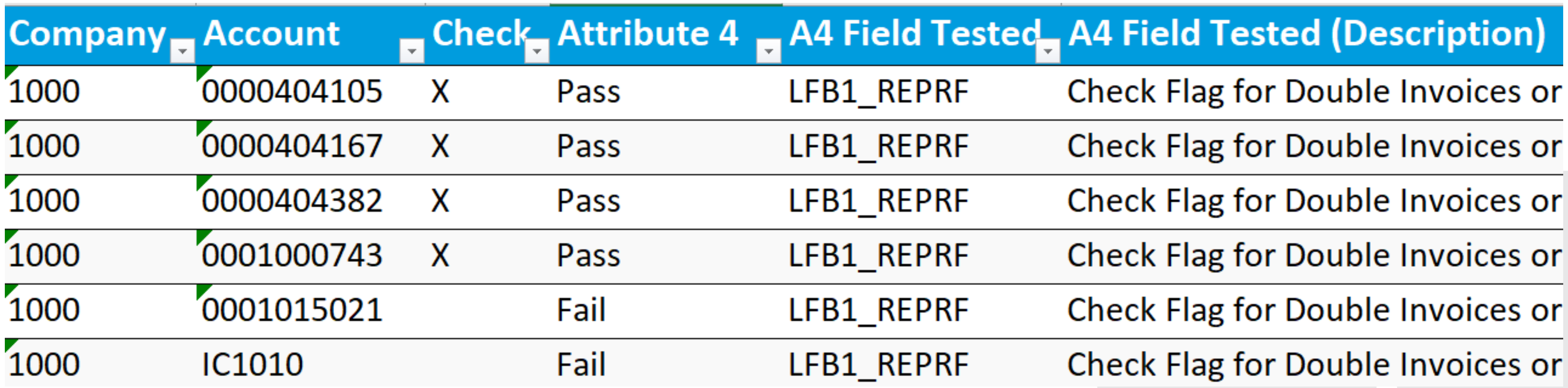
# Automatically generated reports reduce manual effort



| Process Area | Control Description | Conclusion | Table Extract Date |
|---|---|---|---|
| Source to Pay (STP) | Duplicate Invoice Check has been enabled. | Exception Noted | 08-21-2023 |



| Test | Attribute Name | Pass | Fail |
|---|---|---|---|
| 1 | Check company code configured | 7 | 0 |
| 2 | Check invoice date configured | 7 | 0 |
| 3 | Check reference number configured | 7 | 0 |
| 4 | Flag for double invoices or credit memos enabled | 20,044 | 8,539 |
| 5 | Error messages properly configured | 0 | 4 |
| 6 | Double invoice validation field set to required | 0 | 8 |



| Company | Account | Check | Attribute 4 | A4 Field Tested | A4 Field Tested (Description) |
|---|---|---|---|---|---|
| 1000 | 0000404105 | X | Pass | LFB1_REPRF | Check Flag for Double Invoices or |
| 1000 | 0000404167 | X | Pass | LFB1_REPRF | Check Flag for Double Invoices or |
| 1000 | 0000404382 | X | Pass | LFB1_REPRF | Check Flag for Double Invoices or |
| 1000 | 0001000743 | X | Pass | LFB1_REPRF | Check Flag for Double Invoices or |
| 1000 | 0001015021 | | Fail | LFB1_REPRF | Check Flag for Double Invoices or |
| 1000 | IC1010 | | Fail | LFB1_REPRF | Check Flag for Double Invoices or |

# Example RPA/automation use cases

| | IT risk | Business risk | Compliance risk |
|---|---|---|---|
| | **Reusable task bots can be leveraged to perform manual, repetitive and time-consuming tasks. Examples include:** | | |
| **Task Automation**<br>Assists a person in performing repetitive tasks<br>Tasks that have....<br>• Clear (yes/no) business rules<br>• Structured data<br>• Clearly defined steps/can be documented | • Data Comparison Utilities/Report Validation *(e.g., compare two snapshots of the same parameter file or security report)*<br>• Evidence Collection *(e.g., collect data to support IT audits)*<br>• Data Cleansing/Data Wrangling | • Collect data from publically available sources *(e.g., interest rates)* for audit procedures<br>• Audit workpaper preparations<br>• Issues management and reporting<br>• Resource Management<br>• Budget vs. Actual comparison | • Creation or Roll Forward of Audit Testing Lead Sheets<br>• Evidence Collection<br>• Reporting<br>• Continuous Monitoring and Testing<br>• Take Screenshot of evidence |
| | **Process bots can be leveraged to supplement human labor. Focusing human talent on more value added activities** | | |
| **Process Automation**<br>Automates all or part of an end-to-end process<br>End to end audit and controls process that have..<br>• Clear (yes/no) business rules<br>• Structured data<br>• Clearly defined steps/can be documented | • IT Application Controls Validation *(e.g., 3-way match configuration controls, UARs, change control)*<br>• Database and O/S Compliance Monitoring<br>• IT Controls Performance *(e.g., UAR)*<br>• ITGC Testing *(e.g. Change Mgt.)*<br>• IT Configuration Testing | • Manual journal entry Invoice testing *(data extraction, evidence collection, completeness and accuracy validation, workpaper creation)*<br>• Reconciliation control performance<br>• Revenue recognition controls performance *(reconciliation of shipment information vs carrier website data)* | • AML Compliance Automation<br>  • OFAC Search and Update<br>  • 314 Listing<br>  • World Check Search<br>  • Negative News Search<br>• Insurance Compliance Reporting |
| | **Bots that can be leveraged to perform activities that require some level of judgment** | | |
| **Intelligent Automation**<br>Learns and thinks like a person<br>A combination of technologies that...<br>• Extends basic automation capabilities<br>• Works with Unstructured and semi-structured data<br>• Requires capabilities outside of traditional RPA (e.g., AI, NLP, etc.) | • Conversion of unstructured or semi-structured scanned PDF documents to structured text that can be further processes and/or analyzed (e.g., change management evidence) | • Conversion of unstructured or semi-structured scanned PDF documents to structured text that can be further processes and/or analyzed (e.g., vendor invoices) | • Similar use cases plus....<br>• Contract review/key word search<br>• Fair lending analysis and reporting |

**RPA/Automation can drive improvements by enhancing the quality, accelerating the speed and expanding the coverage of risk processes.**

RSM

# Ultimate goal: risk and regulatory compliance platform

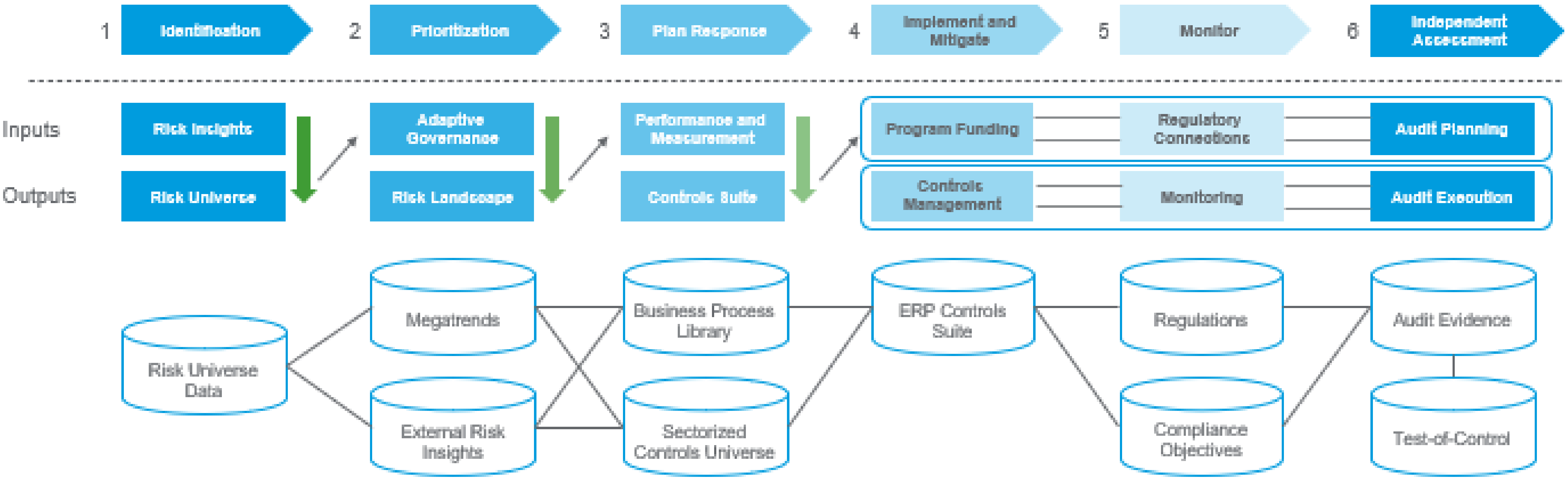
## Linking systems and data management (APIs, GRC platforms and aspirations)

### Connectivity Across the Lines-of-Defense

The real power of Risk and Compliance Management will be interconnectivity between existing GRC systems. There is currently no strong connection between identification of the different types of risk and the existing GRC programs that manage controls downstream:

### Areas of Connectivity Needed

1. Connect Risk Landscape to external insights and perspectives.
2. Connect Risk Landscape to Controls Platform dynamically
3. Connect Monitoring Systems to Audit & Compliance tools



1 Identification

2 Prioritization

3 Plan Response

4 Implement and Mitigate

5 Monitor

6 Independent Assessment

Inputs

Outputs

Risk Insights

Risk Universe

Adaptive Governance

Risk Landscape

Performance and Measurement

Controls Suite

Program Funding

Regulatory Connections

Audit Planning

Controls Management

Monitoring

Audit Execution

Risk Universe Data

Megatrends

External Risk Insights

Business Process Library

Sectorized Controls Universe

ERP Controls Suite

Regulations

Compliance Objectives

Audit Evidence

Test-of-Control

# Key goals of a valued risk and regulatory compliance function

### Horizon scanning

Create the ability to look into the future and identify risk and regulatory compliance that will Impact the organization.

### Provide information

Bring relevant insight to executive management about risks and regulatory compliance needs for better decision-making processes.

### Response

Have systems and processes and technology in place that allow for an efficient and effective response to risk and regulatory compliance needs.

### Analytics

Build the capability to take unstructured and structured internal and external data sources to determine cause and effect relationships for management.

### Culture

Create a risk management culture that instill efficient embedded activities into business processes to manage risk and regulatory compliance.

### Communication/reporting

Create a cascading communication system that provides the right amount of detail at each level of management while providing drill down capability.

# Wrap up and Q&A

RSM

# Thank you

RSM

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute assurance, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services.  This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent assurance, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.