Aaron
One of the
RSM team

RSM

Automation webcast series:
Risk automation

Agenda

- Introductions
- Overview
- Benefits to the risk function
- Use cases
- Taking the next step

With you today

Steve Biskie

Principal, National Risk Automation Leader

- 25+ years of experience in the compliance and internal/external internal audit roles
- Thought leader in the internal audit analytics and continuous monitoring space
- Has helped organizations ranging in size from the mid-market to the Fortune 10 both implement and optimize the use of technology for risk management, compliance, and internal audit-related activities
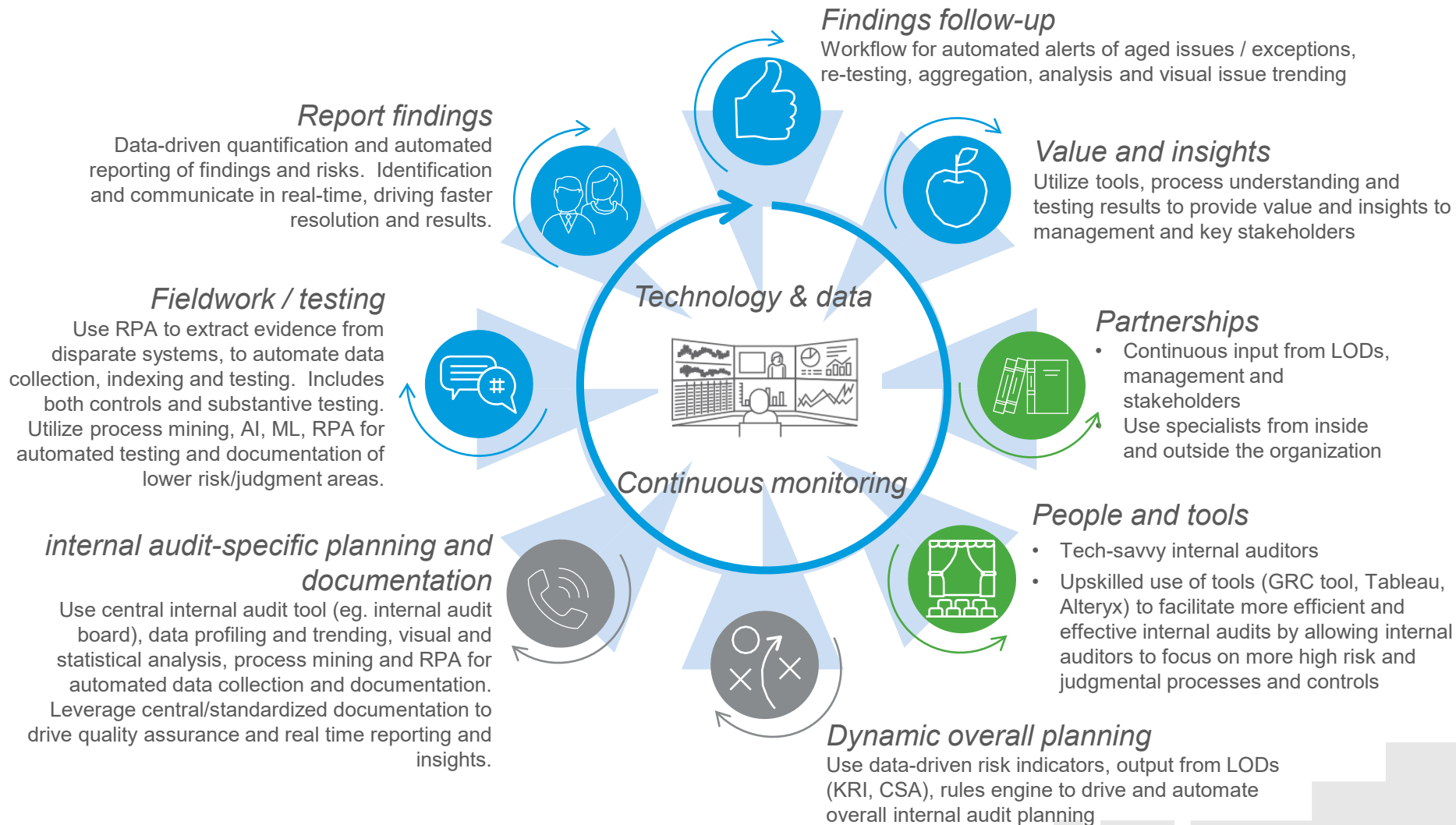
Jake Ryan

Manager, ERP Risk & Automation Services

- 7+ years of experience in IT internal audit, risk automation and data analytics roles
- Focus on digital transformation in client risk functions, identifying and implementing process improvements with RPA and analytics
- Leads a specialized team that designs and develops bots and process workflows using tools such as Alteryx and UiPath

Digitizing the modern internal audit

Findings follow-up
Workflow for automated alerts of aged issues / exceptions, re-testing, aggregation, analysis and visual issue trending

Report findings
Data-driven quantification and automated reporting of findings and risks. Identification and communicate in real-time, driving faster resolution and results.

Value and insights
Utilize tools, process understanding and testing results to provide value and insights to management and key stakeholders

Fieldwork / testing
Use RPA to extract evidence from disparate systems, to automate data collection, indexing and testing. Includes both controls and substantive testing. Utilize process mining, AI, ML, RPA for automated testing and documentation of lower risk/judgment areas.

Technology & data

Continuous monitoring

Partnerships
• Continuous input from LODs, management and stakeholders
Use specialists from inside and outside the organization

internal audit-specific planning and documentation
Use central internal audit tool (eg. internal audit board), data profiling and trending, visual and statistical analysis, process mining and RPA for automated data collection and documentation. Leverage central/standardized documentation to drive quality assurance and real time reporting and insights.

People and tools
• Tech-savvy internal auditors
• Upskilled use of tools (GRC tool, Tableau, Alteryx) to facilitate more efficient and effective internal audits by allowing internal auditors to focus on more high risk and judgmental processes and controls

Dynamic overall planning
Use data-driven risk indicators, output from LODs (KRI, CSA), rules engine to drive and automate overall internal audit planning

Technology & data

• *Anticipate and drive overall risk assessment, internal audit plan and internal audit scope*

• *Source data, metrics catalog, triggers for breaches, alerting*

• *Automated data gathering to support real-time risk monitoring, assessment, tracking and testing*

• *Automate testing of standard processes and controls*

• *Event-driven dashboards for alerts and metrics trends*

Continuous monitoring

• *Use metrics (KPI/KRI) and data-driven triggers to identify emerging risks*

• *Monitor via dashboards / alerts / work queues*

• *Use workflows to auto-create issue documentation,*

• *Identify areas for targeted internal audits*

Why automate in the risk function?

Automation, if implemented effectively, **drives down the cost** of compliance and drives the narrative that internal audit does not have to always be a COST center

Done well, automation can also make your risk management functions more effective by **examining full populations** (instead of samples), and identifying potential issues in **near real-time**.

We want to add value through **rationalizing compliance** activities, **optimizing business processes** and **delivering impactful and effective information** to key stakeholders throughout the business.

Automation for risk
assessment & planning

Key to 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.

Automation of
control performance

RSM

Use case example

Alteryx – facilitation of user access reviews

- Directly supports security and user access principles, can be automated to prevent tedious follow-ups, missed reviews, internal audit issues, etc.

- Directly inform business managers / IT owners if access issues stem from other reviews

- IT owners can be made aware of custom roles/access components that are not being used or are used abundantly to drive onboarding and user provisioning most effectively

- Automate timeliness of reviews for compliance benefit

- Risk personas w/ benefit -
  - Security
  - IT owners
  - Business managers

Use case example

Continuous monitoring & internal audit platforms

- Automation/analytics to consistently update KPIs/KRIs as evidenced through operational internal audits.

- These can support the business through various KRIs that internal audit overlays in risk assessments and cost/benefit analyses

- Third party risk management
  - Identify product categories for cost savings potential
  - Identify trends in bulk purchases, rebates, discounts, etc.

- Automated application configuration
  - Benchmark configurations to automatically detect changes and narrow the timeframe of potential issue / remediation efforts
  - Insights into how business processes change
  - Ability to help various business locations conform to a standardized process

Automation of
control testing

Use case example 1

SAP BASIS validation testing & continuous risk monitoring

Problem Statement: Our client's second Line of Defense identified a gap where no monitoring or validation was being performed internally, and the business was extremely reactive based on the external internal auditor's testing procedures.

Value of Automation: Improved risk coverage, continuous monitoring, proactive analysis of the SAP BASIS environment, promoting the company's innovation strategy through the use of new technology

Use case process flow

Execute ABAP Script to pull all required SAP Data

↓

Aggregate and Transform extracts, processing test logic along the way

Output results in Excel reporting format ↔ Upload files to centralized database for Tableau dashboard reporting

Tool stack

alteryx + tableau
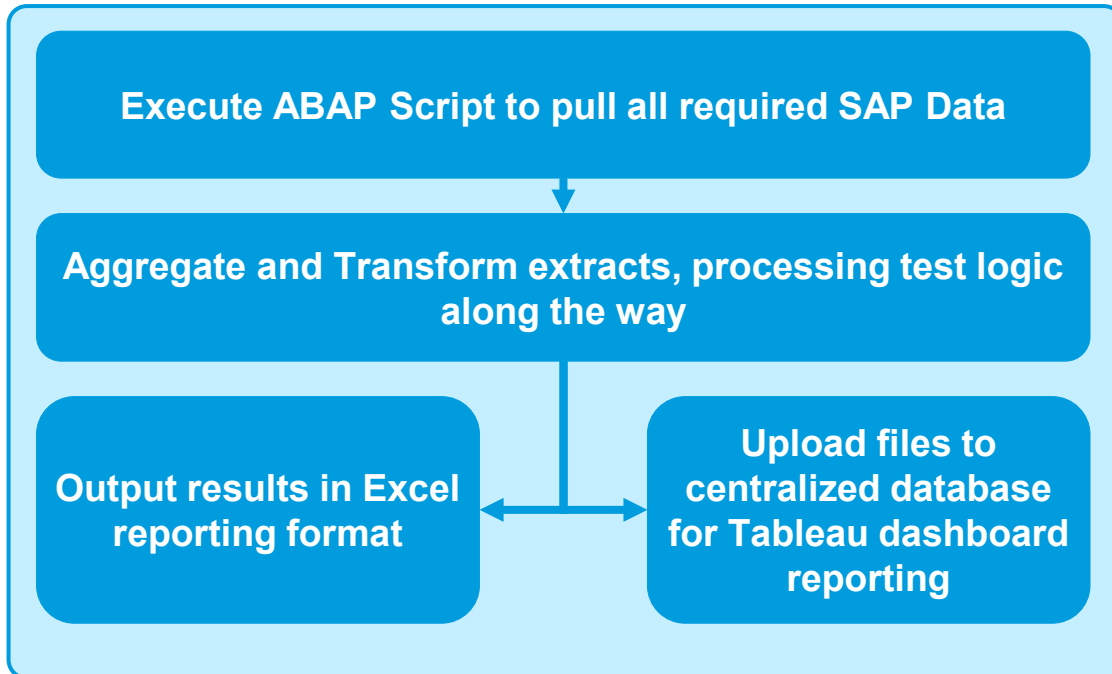
Value area	Current state	Automation state
Coverage	No Independent SAP BASIS testing procedures	80+ testing attributes, independently tested
Frequency	Annual – by externals	Continuous/weekly
Time savings*	40+ providing evidence and remediation	~0.5 to process 80+ Tests for 3 instances of SAP
Risk I identification	Reactive – additional time needed to identify potential or known defects	Proactive – near real-time identification at scale of potential or known defects
Defect remediation	Responding to requests and information from external internal audit	Automated & workflow-based notifications, reminders, access administration

Use case example 2

AWS configuration controls – testing & documentation

Problem statement: *A new internal audit test program introduced for Amazon Web Services required an increase in resource utilization that was not available.*

Value of automation: *Improved risk coverage, continuous monitoring, significant reduction in manual effort.*

Lessons learned: *RPA typically works best on use cases that have already been defined and established.*

Use case process flow

- Access AWS console via Python API in UiPath
- Export in-scope data and store in SQL internal audit database
- Update continuous monitoring dashboard using Tableau
- Process data with control testing logic and produce workpaper output
- Zip workpapers and upload to TeamMate+

Tool stack

UiPath | python | Microsoft SQL Server | tableau
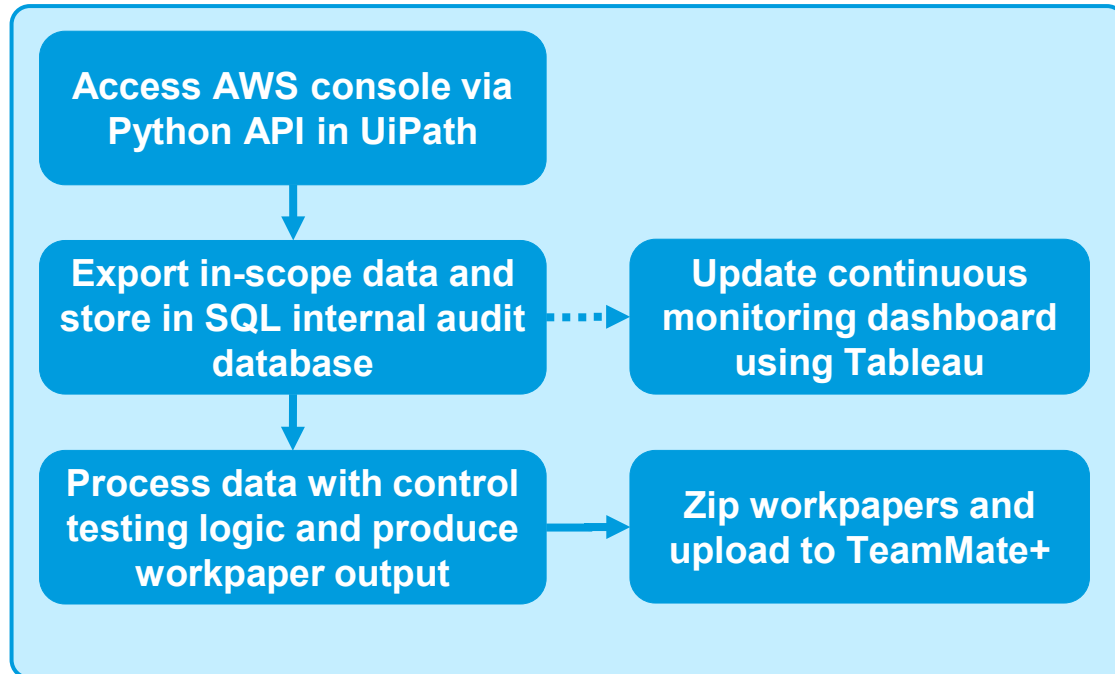
Value area	Current state	Automation state
Coverage	Sample of 10-15 Instances	80+ in-scope Instances
Frequency	Bi-annually	Weekly
Time savings*	~24 hours per instance	~0.5 hours per instance
Strategy	Start of automation journey – start of organizational learning	Automation-driven, team seeking new use cases actively
Standardization	Testing would be documented differently by tester, and requested data may differ instance to instance	Standardized procedures promotes simpler review steps and promotes more analytic capabilities
Scaling	Various cloud internal audits are expected to operate and report separately	Allows for other cloud internal audits to integrate more smoothly into the new framework

Use case example 3

SQL privileged access – testing & documentation

Problem statement: The IT business controls team conducted SQL database privileged access testing once a year for a sample of SQL DBs. This cumbersome process required over 140 hours of manual data extraction and analysis and provided risk coverage over .02% of the population of SQL DBs.

Value of automation: Improved risk coverage, continuous monitoring, significant reduction in manual effort.

Use case process flow

- **Extract permissions from SQL DB instance**
- **Aggregate and transform extracts for optimized analytics**
- **Integrate data from AD & HR sources to support analysis**
- **Identify potential or known instances of excessive access via logical indicators**
- **Prepare output report for review with key risk indicators**

Tool stack

UiPath   Power BI
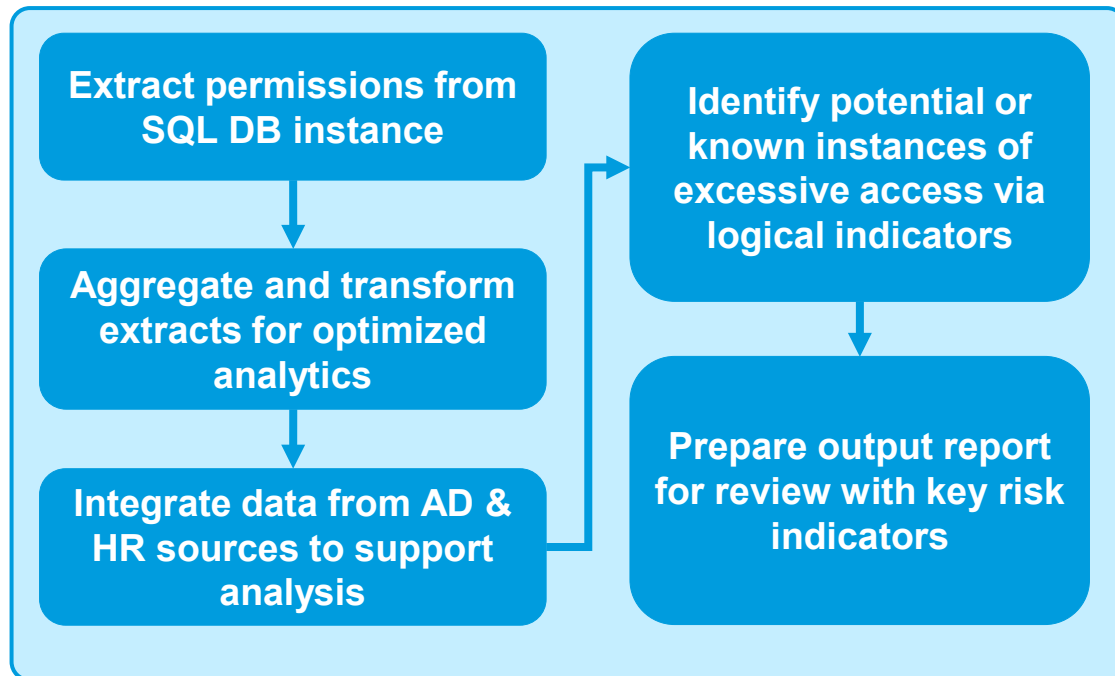
Value area	Current state	Automation state
Coverage	Sample of ~ 35 databases	5,000+ SQL databases
Frequency	Annual	Continuous/weekly
Time savings*	~4 hours per DB	~0.2 hours per DB
Risk identification	Reactive – additional time needed to identify potential or known defects	Proactive – near real-time identification at scale of potential or known defects
Defect remediation	Email notifications, human-triggered reminders, manual IT requests	Automated & workflow-based notifications, reminders, access administration
Regulatory impact	Limited runway to address defects in advance of regulatory assessments	Continuous compliance

Automation of internal audit support activities

Use case example

UiPath – evidence & data extraction for internal auditors

- Give time back to the business by automatically generating or extracting data with compliance requirements fulfilled (I.e. completeness and accuracy, timeliness, screenshots, etc.)

- Ensure all evidence extracted is correct the first time

- Take it further:
  - Even have the bot or APIs upload these directly to a GRC tool such as internal auditBoard, Workiva, Archer, etc.
  - Have the evidence directly loaded into the workpaper or lead sheet based on your organization's readiness
  - Work with IT owners to create tagging options to tag transports/change documents/etc. directly with ticketing system tools to help remove search time for IT and other app owners looking for follow-up evidence
  - Potential for 100% testing and/or continuous monitoring

Use case example

Alteryx – internal auditBoard data & file extraction

- Maximize the use of your GRC tool data by exporting your information with Alteryx and APIs

- Integrate your GRC tool data directly with data visualization tools like Tableau or Power BI

- Take it further:

    - Even have the bot or APIs upload these directly to a GRC tool such as internal auditBoard, Workiva, Archer, etc.

    - Have the evidence directly loaded into the workpaper or lead sheet based on your organization's readiness

    - Work with IT owners to create tagging options to tag transports/change documents/etc. directly with ticketing system tools to help remove search time for IT and other app owners looking for follow-up evidence

    - Potential for 100% testing and/or continuous monitoring

Automation in practice

Demo: journal entry testing bot

Manual journal entry testing can be a cumbersome task, leading to lots of sample requests, individual follow-up, and manual testing procedures.

Automating this process leads to improved testing accuracy, time returned to the internal auditor, and enables the potential for enhancements such as continuous monitoring.

Taking the next step

Where to start

- Think about what's going to get management most excited
  - What are the internal audit Committee's top concerns?
  - Is IT not providing business champions what they need?
- Don't be afraid to fail hard, fail fast
- Start small – select a manageable pilot use case
- Do your research
  - There are many different tools and approaches you can take

What doesn't work

- Going into this 'digital transformation' without buy-in from all stakeholders
  - Show the benefit
  - Remove the blockers
- Lack of due diligence
  - Understand the big picture
  - Ensure the people, processes, and technology related to automation efforts are considered
- Lack of active monitoring
  - Utilize KPIs/KRIs with true quantitative metrics

Things to caution

- You may not get it right the first time
- Change is the name of the game
  - People will get new skillsets
  - Technology and system changes
  - Processes may already be the most optimized, or just can't realistically be modified for automation
  - Change takes time
- Compliance impacts
  - Bias in AI/automation
    - e.g. analyzing resumes

Automation identification methods

Opportunity scan
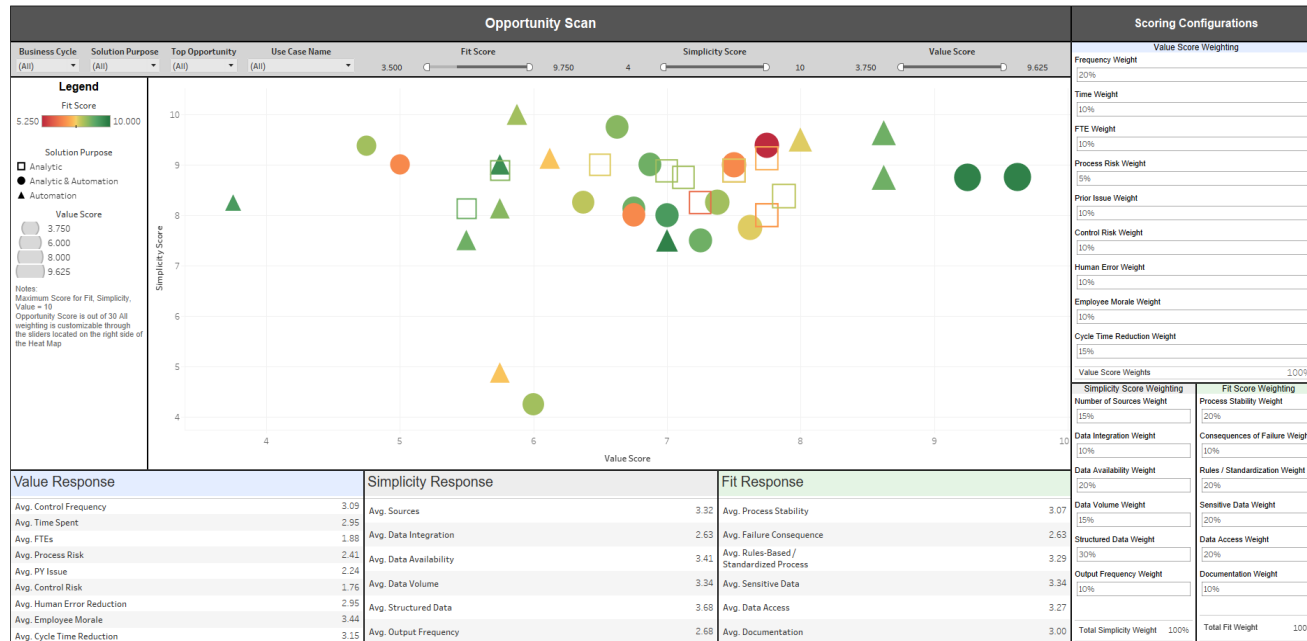
Process mining
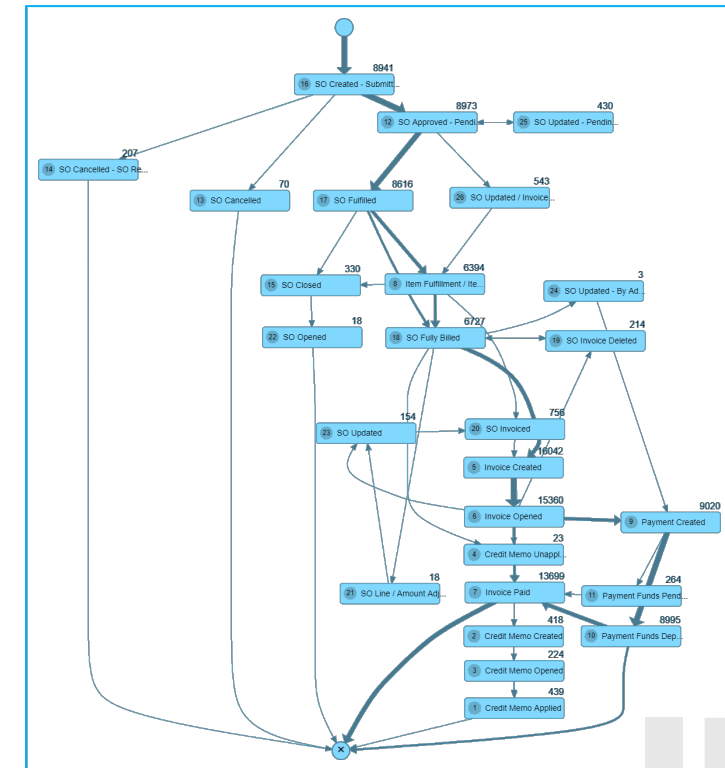
Q & A

Thank you

Contact us

Steve Biskie

Principal, National Risk Automation Leader

- Email: steve.biskie@rsmus.com
- Phone Number: (303) – 298 – 6503

Jake Ryan

Manager, ERP Risk & Automation Services

- Email: jake.ryan@rsmus.com
- Phone Number: (614) – 499 – 7944

THE POWER OF BEING UNDERSTOOD
ASSURANCE | TAX | CONSULTING