



Audit and AI

RSM Risk Consulting

November 21, 2023

Speaker

Dave Mahoney

Director, Security and Privacy Risk
Blue Bell, Pennsylvania
dave.mahoney@rsmus.com
+1 610 731 4609



Background

As the Go-to-Market Director for Cyber Transformation Services at RSM, my responsibilities include raising global awareness of our services. I work to ensure that we provide comprehensive cyber risk consulting to our clients by leveraging the full range of RSM's capabilities.

I have over 20 years of professional experience in cyber information technology, organizational change, and executive alignment. I provide technology and business process transformation services to my client base. I drive organizational change through innovative future state design, target operating model development, functional strategy alignment, and complex implementations.

Professional affiliations and credentials

Certified Information Systems Security Professional (CISSP)

Education

Bachelor of Science, Strayer University

Polling Question

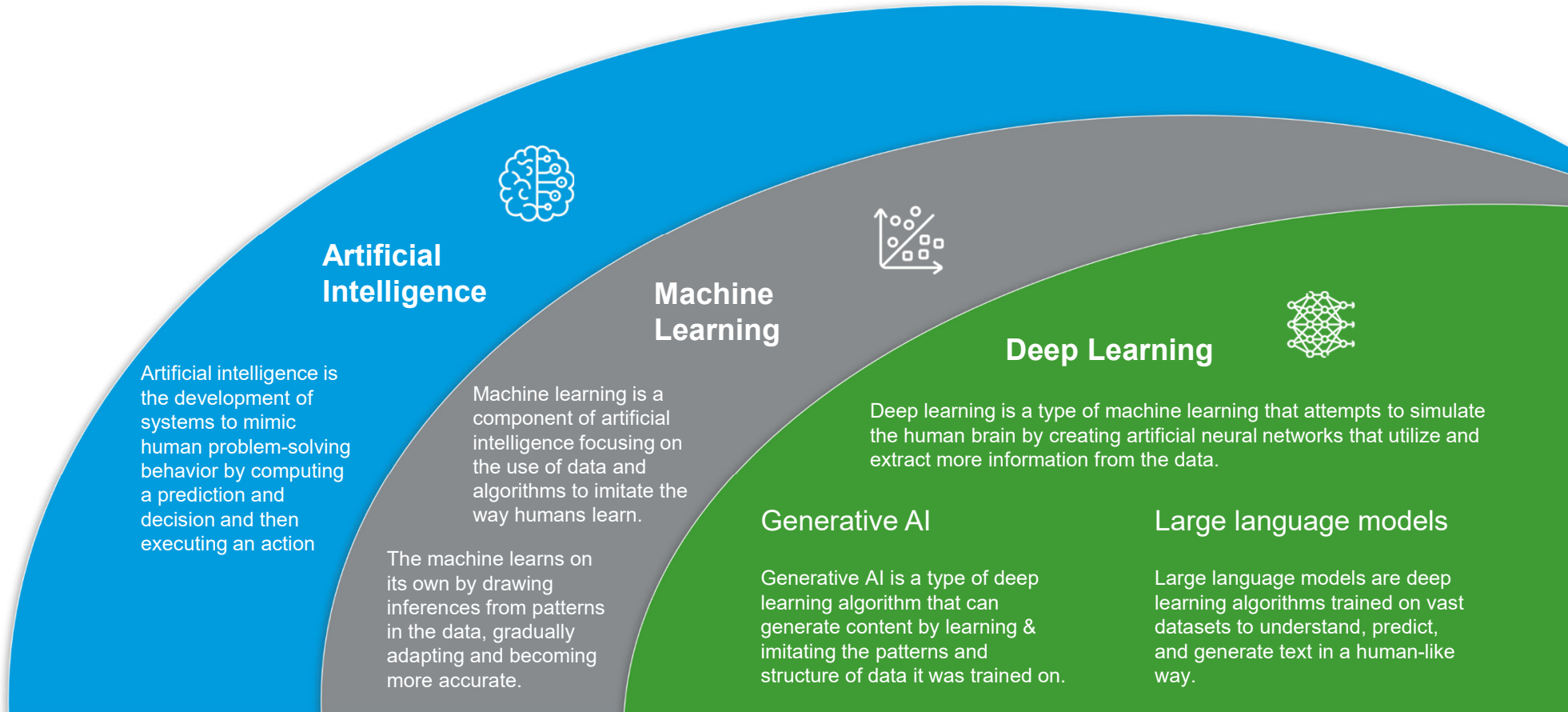
What is your function within your organization?

AGENDA

1. AI Landscape
2. AI Journey
3. Risk and Safeguards
4. Using ChatGPT at work
5. How AI can enhance internal audit function



Artificial Intelligence Landscape



Artificial Intelligence

Artificial intelligence is the development of systems to mimic human problem-solving behavior by computing a prediction and decision and then executing an action



Machine Learning

Machine learning is a component of artificial intelligence focusing on the use of data and algorithms to imitate the way humans learn.

The machine learns on its own by drawing inferences from patterns in the data, gradually adapting and becoming more accurate.



Deep Learning

Deep learning is a type of machine learning that attempts to simulate the human brain by creating artificial neural networks that utilize and extract more information from the data.

Generative AI

Generative AI is a type of deep learning algorithm that can generate content by learning & imitating the patterns and structure of data it was trained on.

Large language models

Large language models are deep learning algorithms trained on vast datasets to understand, predict, and generate text in a human-like way.

Polling Question

Approximately when did the practical field of study called Artificial Intelligence begin:

1850

2010

1956

1994

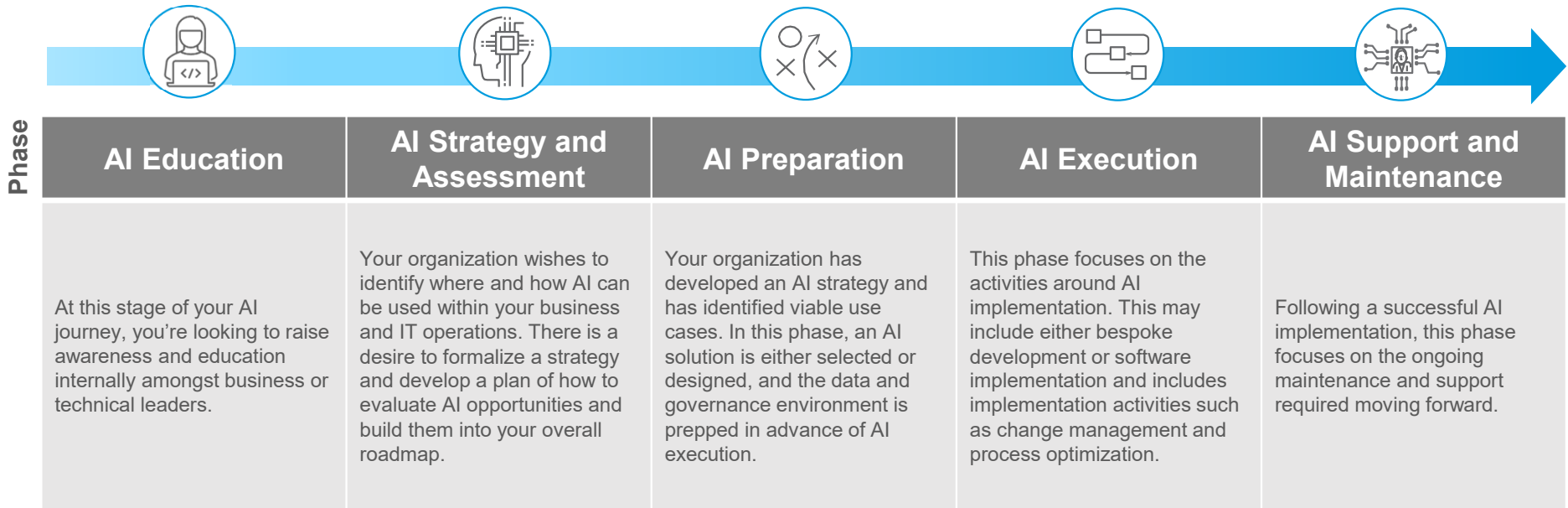


Enterprise Journey

November 21, 2023

JOURNEY

AI customer journey outlines a strategic pathway for clients to harness the potential of AI at all phases. RSM can help you navigate this journey from initial education through to the implementation of tailored AI solutions. We support our clients not just with successful adoption, but also the ability to make impactful decisions and ultimately become AI champions within your organization. Specific offerings by customer journey phase are outlined in the following slide.



Polling Question

Where is your organization in the AI Journey?

Education

Strategy & Assessment

Preparation

Execution

Support and Maintenance (Multiple Production Systems)



Risks and Safeguards

November 21, 2023

Risks and Safeguards for AI Applications

Understanding multi-dimensional AI-related risks – *regulatory, privacy, legal, ethical, operational, and financial* - is vital for smooth implementation, responsible use, trusted results, and compliance.

	01 End User	02 Product	03 Provider	04 Model
	Users or AI agents using and prompting AI products	AI-based apps, like ChatGPT, that take prompts and automate content generation	Developers and access providers to an AI model (e.g., OpenAI, MS Azure, AWS, Google)	Advanced ML models that interact and respond like humans (e.g., GPT, Claude)
RISKS	<ul style="list-style-type: none"> Misinterpretation of output Overreliance on model output Prompt hijacking Sharing sensitive data 	<ul style="list-style-type: none"> Exposure of sensitive data Bugs, defects or malfunctions Misconfiguration Unexplainable results 	<ul style="list-style-type: none"> Data breach Corporate data leakage into training data Model unavailable due to GPU shortage 	<ul style="list-style-type: none"> Limited training data / obsolete Unpredictable output Inaccurate & Biased outputs Model performance drift
SAFEGUARDS	<ul style="list-style-type: none"> User education / training Application input controls Output verification Data loss prevention alerts “Acceptable Use” policy Data handling protocols 	<ul style="list-style-type: none"> DevSecOps practices Data encryption, tokenization / data masking User access & entitlements Periodic security reviews Change control Application monitoring 	<ul style="list-style-type: none"> Third-party Risk Assessment License agreement, terms and conditions SOC report Service Level Agreements 	<ul style="list-style-type: none"> Performance testing against standard test dataset Development documentation and release notes Red Team pressure testing User feedback
Cross Company: AI Policy Model Risk Management Employee Communication Culture of Accountability Feedback Channels				

Trustworthy and Responsible AI Solutions

Implementing AI in requires a strategic combination of automated safeguards, human oversight, and layered defense to ensure reliable, trustworthy operation.



01

Accurate

Produce correct and trustworthy results

02

Transparent & Explainable

Clear understanding of how models operate and explain their decisions

03

Reliable

Consistent performance over time

04

Robust

Protection against manipulation and ability to handle unexpected inputs

05

Fair

Mitigating biases to avoid discrimination

06

Secure & Private

Safeguarding sensitive data and protect from unauthorized access and malicious attacks

07

Resilient

Ability to recover and adapt to changes or failures

08

User Control

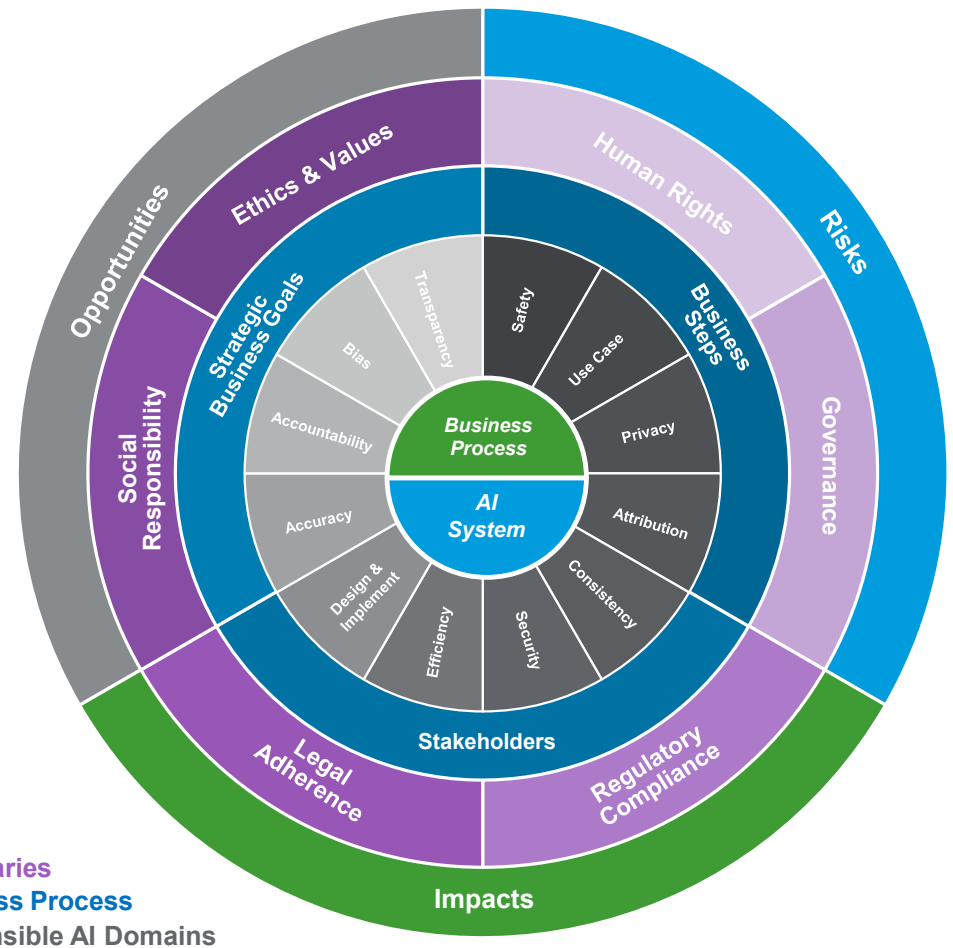
Empowering users with ability to decide when and how AI is applied

IT Infrastructure | Application Controls | Risk Assessment | Human-in-the-Loop | Evaluation and Monitoring | Education and Awareness

Responsible Governance Framework

Our Solution to Existing Framework Challenges:

- System-centric without involving the business process
- Minimum coverage regarding the impact of Third-party systems
 - Supply Chain
 - Partner Ecosystem
 - Vendor Ecosystem
- Misappropriation of trends as internal/external data bias
- RSM created a unified Enterprise Risk Management Framework by which to govern AI from inception through operations



Polling Question

The governance scope of AI systems must include (choose two):

AI System Design

Data Privacy

Technical Controls

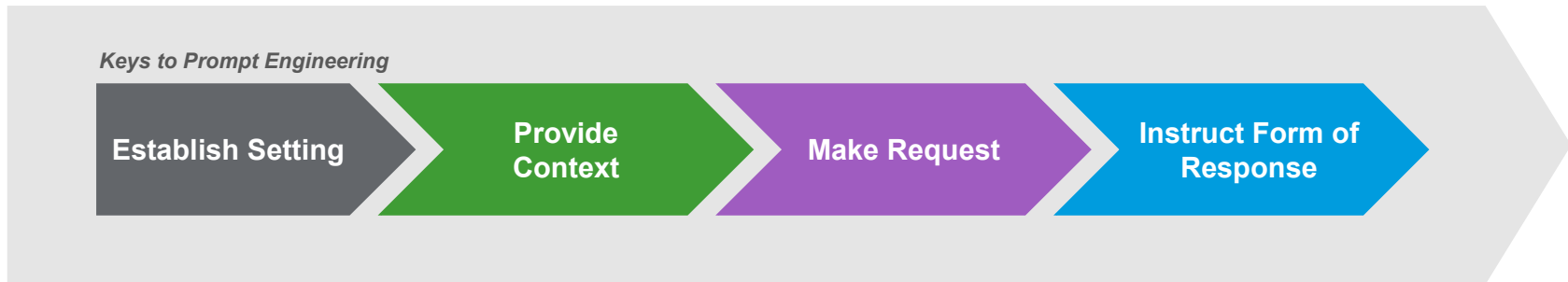
Business Process



Using Opensource AI: Do more, faster

November 21, 2023

Prompt Engineering



Establish Setting	Provide Context	Make Request	Instruct Form of Response
<ul style="list-style-type: none"> Describe the situation and setting behind the prompt <i>"I am an Auditor monitoring the construction of a broadband network."</i> 	<ul style="list-style-type: none"> Provide the detail surrounding the specific prompt request <i>"I am writing a narrative detailing the network validation audit procedures we conduct. This will be the cover sheet before sharing findings. Here are the procedures we will conduct [insert procedures]."</i> 	<ul style="list-style-type: none"> Request what you'd like analyzed or produced <i>"Please summarize the procedures in narrative form. Ensure all procedures are represented in the narrative output. Provide 3 options of introductory paragraphs to choose from."</i> 	<ul style="list-style-type: none"> Describe what form the output should be in <i>"Please write the narrative in 500 words and 3 paragraphs. Use a professional, concise, and informative tone."</i>

Opensource AI Use Cases

EXCEL SOLUTIONS

- Draft Excel formulas and suggest solutions
 - Write a formula to match Table 1 “Last, First” name with Table 2 “Last, First Middle” name
 - Please provide formula to conditionally format values in List 1 that are not in List 2
 - I’d like to extract the values from cells A1 and B1 from every tab in my workbook, what’s the best way to do that?



ORGANIZATION

- Organize notes for report writing, speeches, and emails
 - Can you organize my notes for a speech on AI in Internal Audit into paragraphs and bullet points? Suggest 5 likely questions the audience may ask.
 - What are the 3 most important takeaways from this article?

BRAINSTORMING

- Conversationally explore ideas
 - I’m designing a monitoring for a payment card institution, what are some program risks I should be aware of?
 - What documents could I gather to monitor the progress of a water infrastructure construction project?

RESEARCH

- Research copilot when learning technical industry and regulatory information
 - I’m reading about the benefits of fiber vs. coaxial cable in broadband construction, can you compare the advantages and disadvantages of each?
 - Does Section 106 relate to GEFA or GHPA? What are the key compliance requirements to monitor?

Polling Question

ChatGPT can be a useful tool. It can be more useful when provided:

Excel Data

Images

Specific Prompt

Sensitive Information



AI Enhancing Internal Audit

November 21, 2023

General AI/ML Use Cases for Any Internal Audit Function



Audit execution can be improved by fully embedding AI, automation, and 'traditional' analytics across all phases of the internal audit lifecycle – integrating the right models and tools as the situation warrants.



01 Develop Audit Plan

- Suggest risk interview questions and distribute risk questionnaires to risk owners
- Theme unstructured interview comments from risk owners and stakeholders
- Summarize 1st/2nd line KRIs and management CSAs for suggestions and Continuous Risk Assessment
- Summarize changes in people (HR data), processes (procedure docs), and technology (configuration data)

02 Plan the Audit

- Theme and quantify employee complaints to detect emerging risks and trends
- Produce detailed lists of compliance requirements tailored to a specific (sub)process ★
- Monitor document and meeting requests and follow-up, as necessary
- Analyze process narratives to suggest audit activities, tests, action plans, and risks and controls ★

03 Fieldwork / Testing

- Evaluate call center transcriptions, case management notes, or contract text for compliance
- Suggest analytical procedures and business rules based on data available in a data file
- Generate (or explain) analytic code for automating data-driven audit tests
- Generate work paper content and provide first round review of workpaper quality

04 Reporting

- Dynamic report narrative generation of risks, issues, and action plans
- Auto-annotate dashboard tables and visualizations to enhance interpretation
- Tailor report content to different stakeholders aligned with their interests and comprehension levels
- Associate report findings with associated guidelines and best practice libraries

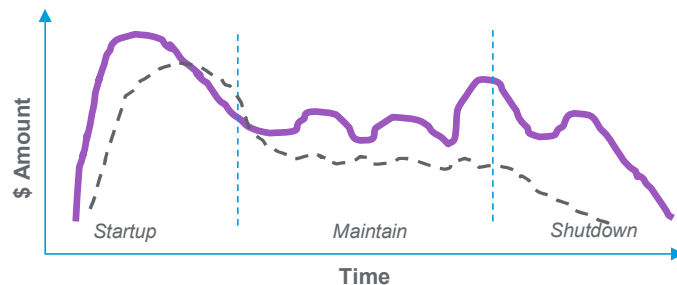
05 Follow-up / Monitoring

- Generate text for automated alerts or service tickets on aged issues/exceptions
- Summarize, integrate, and synthesize results across multiple continuous monitoring apps
- Recommend process improvements based on output of continuous KRI, KPI, and KCI monitoring
- Synthesize scenarios and test data to effectively challenge monitoring logic and rules

Can we detect unusual grant drawdowns over the life of the grant? Are we paying for unallowable expenses?

Grant Lifecycle Analysis

Drawdown Profiling



- Procedures

- Review patterns of drawdown activity
 - Outliers depend on where you are in the lifecycle
- Conduct "profile analysis" comparing drawdown profile to similar grants or standard "ideal" profile

Questioned Costs

Unallowable/Allowable Expenses

- Method 1: Expert Rules
 - 100% review of population using known "if/then" logical rules
- Method 2: Machine Learning
 - Train a classifier on denied costs from prior periods
 - Run trained model on current period data

Problem: Can we highlight “rare flows” or unusual account combinations in the transactional detail of the material accounts we test?

Procedures

- Look back 6 to 12 months
- Iterate through GL detail to determine left and right side of entries
- Cluster account combinations
- Isolate the rare and unusual account for deeper inspection

Problem: Can we detect anomalies in the material accounts we are testing?

Features

- Description, amount, posted by, posted date, related accounts

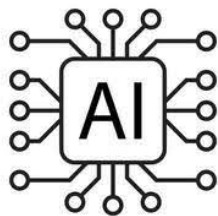
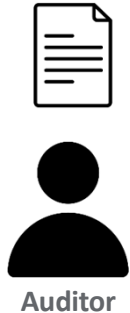
Procedures

- Cluster line items within material accounts based on their statistical similarities
- Flag line items that do not cluster with other items for deeper inspection

Case Study: From Process Narrative to Actionable Insights

GenAI Case Study: Application of GenAI in a large financial institution's Internal Audit function, where it transformed business narratives into risk-enriched process diagrams. Utilizing language models, GenAI can create process flows, link to metrics, and recommend Audit Tasks and Activities, Risk & Controls, Action Plans, and Test Steps.

Standardized Business Process Narrative

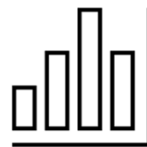
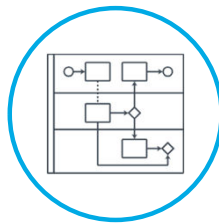


Cognitive Engine

GenAI automation extracts key details from process narratives to generate a Process Flow Diagram



Process Flow Diagram







Metrics



GRC Data



Recommendations (GenAI+GRC Data)

-  **Audit Tasks and Activities**
Generate task/activity plans to address exposures in process
-  **Risks & Controls**
Identify potential risk and control gaps in critical processes
-  **Action Plans**
Generate action plans based on effective plans from prior audits
-  **Test Steps**
Identify potential manual and analytical tests