

datricks

Ensuring Financial Integrity in the Age of GenAI



Contents

Part 1	Why GenAI is more than just a tool	3
	The state of finance and internal audit	
	GenAI changes everything	
	The opportunity for finance leaders	
	The opportunity for internal auditors	
Part 2	Two critical steps to maximizing value	8
	Step 1: adopting the GenAI mindset	
	Step 2: expecting more than a chatbot	
Part 3	The GenAI blueprint for finance and internal audit	13
	The three pillars	
	What to look for	
	Key benefits	
Part 4	GenAI-powered Financial Integrity in action	21

Part 1

GenAI
is more than just a tool
it's a transformation

The state of finance and internal audit

Finance and internal audit leaders and their teams are under immense pressure to protect their organizations from the fallout of exposures resulting from errors, non-compliance, and fraud.








But while the volume and velocity of financial data keeps growing, the tools they rely on – traditional BI, dashboards, and static analytics, can't keep up.

These tools surface what's already happened, often too late, and rarely offer the clarity and foresight needed to act with accuracy and confidence.



GenAI changes everything

GenAI empowers finance and audit teams to overcome these limitations by:

-  **Scanning and analyzing**
massive amounts of structured and unstructured data across systems and processes
-  **Detecting**
patterns
-  **Surfacing**
new, unseen insights
-  **Understanding**
context
-  **Connecting**
dots no human or legacy system can
-  **Delivering**
clear next-best action guidance
-  **Acting autonomously**
when needed

And best of all, it works through simple, conversational language. No code, no technical training. Just ask and get clear, actionable answers.

The GenAI opportunity

For finance leaders

it transforms manual, reactive operations into real-time control and data-fueled, insight-rich leadership.

For internal audit

it replaces sample-based, time-consuming, periodic reviews and reports with always-on compliance and audit readiness.

“

“The technology (GenAI) is rapidly reshaping CFOs' role by offering new opportunities in automation, data analytics and risk management.”

World Economic Forum



“

“The findings of our research show that AI is set to transform internal audit in the next 12 months, with adoption set to double to 80%.”

Walters Kluwer



GenAI is not just another tool

With its autonomous, proactive, and predictive capabilities, GenAI represents a transformational shift.

Without GenAI

Undetected

Exposures from errors, non-compliance, and fraud often remain under the radar.

Hours, days, and weeks

Manual investigation of financial data and processes is a time-intensive and resource-draining task.

Out of reach

Correlating masses of data points across multiple systems and understanding context remains unattainable.

Insufficient

Access to insight depth and ongoing visibility is limited with traditional BI tools, analytics, and dashboards.

THE COST

Missed exposures, lost time, financial leakage.

With GenAI

Revealed

Exposures are surfaced and acted on, as they happen, before the damage is done.

Instant

Data-led and intelligence-driven insights about exposures, anomalies, and trends, are delivered in real time

Effortless

Connecting dots across enterprise systems, processes, data, and exposures is autonomous.

Extensive

Finance gains complete, real-time visibility with deep, connected insights.

THE PAYOFF

Reduced exposures, faster, more efficient operations, and enterprise-wide Financial Integrity.

Part 2

**Two critical steps
to maximizing value**
and capturing the opportunity

Step 1

Adopting the right mindset

When it comes to GenAI, the shift from experimentation to enterprise-wide impact doesn't happen by simply deploying tools and waiting for results.

The first and most critical step is to adopt the right mindset.



By 2026, it's predicted that over 80% of organizations will have employed generative artificial intelligence (GenAI) in some capacity, up from less than 5% in 2023 but only 16% will do it successfully."

**World Economic
Forum**



How to adopt the right mindset

Recognize GenAI's true potential

Embracing the GenAI mindset means understanding that it's a force multiplier. Yes, it helps us do everything faster, but also – better, smarter, with greater precision, and at scale.

Think outside the search bar

GenAI isn't a search engine. It's a strategic partner, proactive doer, and source of deeper insights.

Engage effectively by treating it as a collaborator that helps you uncover the unseen, connect the dots, and even act on its own with intelligence.

Prompt with purpose

To get meaningful output, you need to give meaningful input.

Frame your goals clearly, provide context, and ask thoughtful questions. GenAI rewards clarity with precision and insight.



As McKinsey consistently emphasizes, **mindset shifts are essential** to any successful transformation.

And **adopting GenAI** for productivity, decision-making, and ensuring Financial Integrity, is nothing short of a profound tectonic shift in how finance and audit operates and leads.

Step 2

Expecting more than a chatbot

When you adopt the GenAI mindset you are ready to unlock its full potential for discovering, understanding, correlating, explaining, guiding, and transforming finance and internal audit.

The second step is to expect more than just a chatbot, and to treat it as an always-on, on-demand intelligence layer that's working 24/7 to elevate Financial Integrity.



Part 3

The GenAI blueprint for finance and internal audit

The 3 pillars

The three essential capabilities that form the blueprint for a GenAI-powered transformation of finance and internal audit are:

**Autonomous
process discovery**

**Integrity exposure
detection**

**Integrity
intelligence**



1

Autonomous process discovery

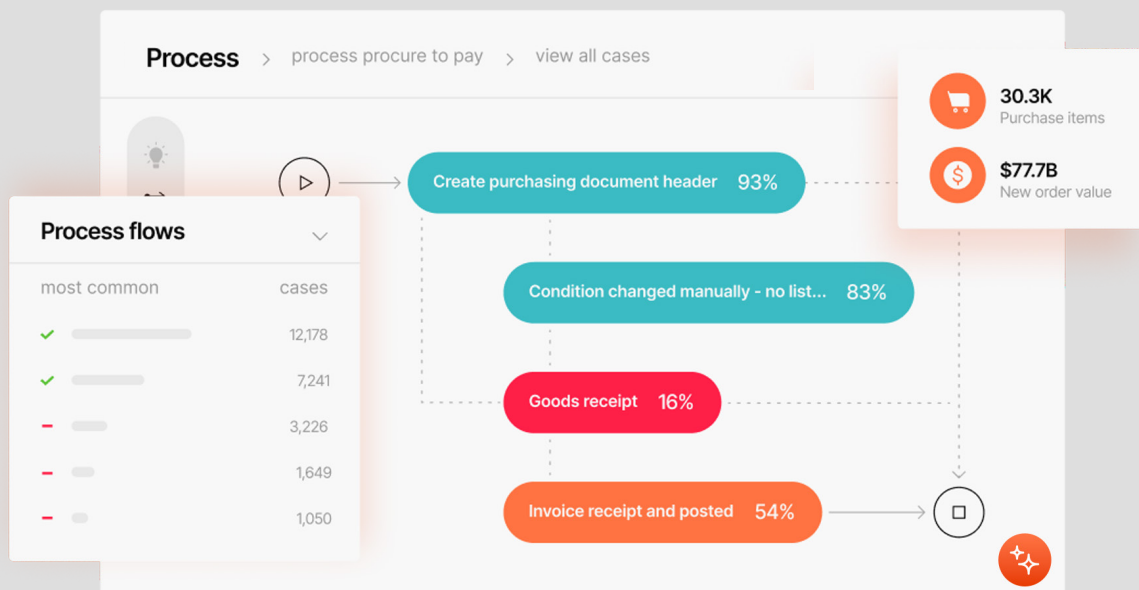
A key capability for elevating Financial Integrity with GenAI is the ability to automatically and continuously map and analyze the organization's financial processes, extracting insights directly from the operational systems that run them, particularly ERP and CRM.

To provide full context, GenAI must enrich its insights by combining signals from across the enterprise with external data sources such as regulatory updates, third-party intelligence, and global newsfeeds.

This is how you can uncover how your business actually runs, where it's exposed, and how emerging trends may impact operations.

Continuously & autonomously

- Mapping and analyzing processes
- Extracting insights from enterprise systems
- Enriching with data from additional sources



2

Integrity exposure detection

Your GenAI should be able to detect discrepancies, compliance gaps, fraud patterns, and anomalies across systems, in real time, both on-demand and without being prompted.

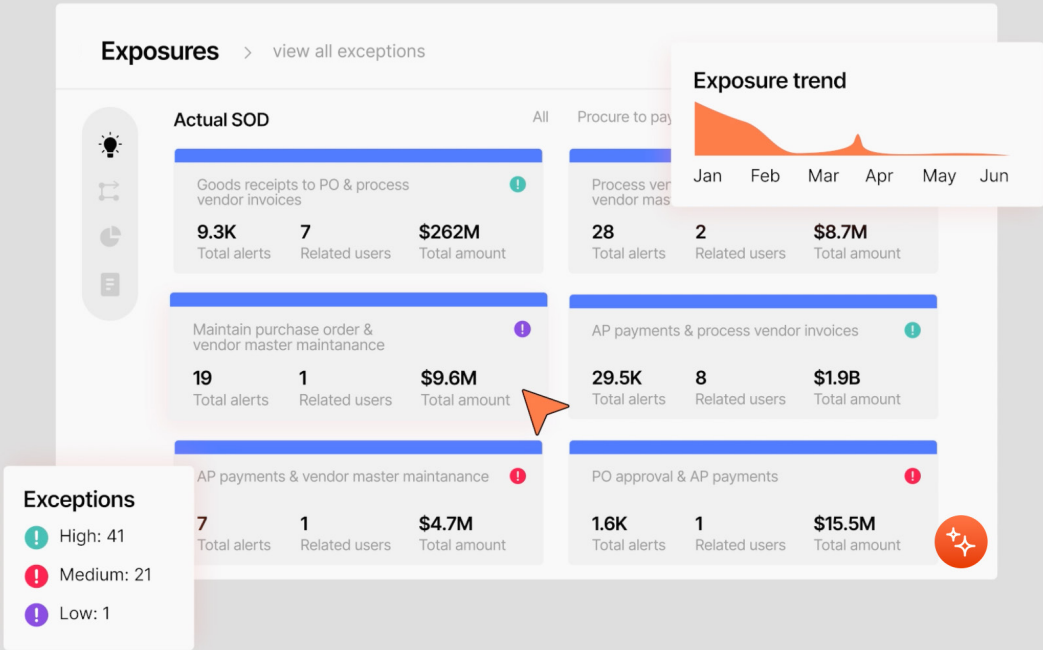
It should connect exposure signals, understand the full context and impact, and proactively flag what matters most.

Prioritization and next-best-action guidance must be built in to ensure that nothing slips through the cracks and that your team always knows where to focus.



Real-time & proactive

- Detecting discrepancies, gaps, patterns
- Connecting exposure signals
- Prioritizing and flagging
- Sending alerts, no prompt required



3

Integrity intelligence

GenAI should also be able to power insight-rich leadership by enabling any question to be asked in natural language, and delivering instant, actionable answers about the what, where, when, and impact of every issue.

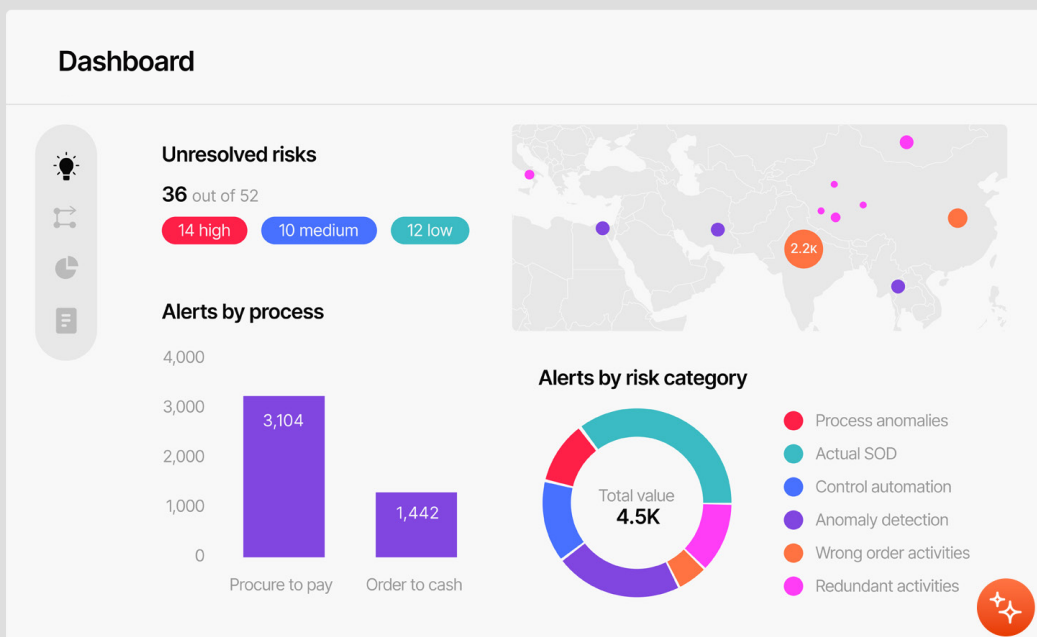
It should enable corrective actions to be taken immediately, either through clear and intuitive guidance or autonomously when appropriate.

This is how finance and audit leaders move from reactive operations to a dynamic control tower, with intelligence-led decisions and elevated Financial Integrity.



Empowering leadership

- Asking questions in plain language
- Getting instant context-rich answers
- Understanding connections
- Gaining complete visibility and control



What to look for

Effortless setup for instant value

To get the most out of GenAI, it should be up and running fast, with minimal effort and no complex data prep.

It should start delivering results in days, not weeks or months.

Moreover, implementation and day-to-day operation shouldn't require coding or specialized skills.

And, the GenAI should be built for finance and internal audit professionals to use independently, in natural language, intuitive and effective for any user.



What to look for AI designed for trust

Especially in the finance and audit domain, AI should be trusted 100%.

It should be explainable, with no training on your data, always enabling human-in-the-loop control.



Data stays secure

All data remains within your environment or a secure, dedicated cloud, e.g., AWS VPC.

No training on your data

Foundation models such as AWS Bedrock with Claude or Azure OpenAI are used, but your proprietary data is never used for training.

Privacy by default

No personally identifiable information (PII) is ever exposed. Conversations are transient, stateless, and never stored.

Full explainability and control

Human-in-the-loop oversight ensures that AI actions are transparent, trackable, and always verifiable.

Key benefits

the power of GenAI for Financial Integrity

When GenAI becomes your always-on intelligence layer, it transforms finance and internal audit operations and drives Financial Integrity across the organization by:



Going beyond analytics & dashboards

with an always on intelligence layer that works 24/7 to detect and prevent the damage of errors, non-compliance, and fraud.



Understanding the full context

of every anomaly, event, and alert and why it matters.



Making sure no issue goes unaddressed

with real-time, proactive notifications that deliver insight, clear corrective guidance, and autonomous



Staying ahead of exposures

with early warnings that drive smart action.



Seeing the unseen and knowing the unknown

with intelligence-led insights that connect the dots across data, systems, and processes.



Increasing team efficiency and capacity

by letting GenAI do the heavy lifting, including investigation, analysis, exposure correlation, prioritization, and taking corrective action autonomously.

Part 4

GenAI-powered Financial Integrity in action

Now that we've explored what GenAI makes possible for finance and internal audit leaders and their teams, it's time to see it in action.

Process with the most critical exposures



User prompt

Which process poses a critical risk?



AI response

The area of greatest financial exposure is the procure-to-pay process, specifically due to purchase order (PO) splitting, where multiple POs are created for the same material and vendor within a short time frame, e.g., under one week.

What this means

This pattern suggests potential circumvention of internal controls, such as approval thresholds or budget limits. In this case, the recurring behavior has been identified in transactions involving John Smith and Lisa Miller.

The screenshot shows a dashboard titled 'Exposures' with various filters and a 'Co-pilot' chat window. The dashboard includes a summary of 40 exposures with 33 high, 6 medium, and 1 low severity alerts, and a total exposure amount of €37.8B. The 'Co-pilot' window displays the user's prompt and the AI's response regarding the procure-to-pay process.

Process	Total Alerts	Related Users	Total Exposure
Goods Receipts to PO & Maintain Purchase Order	54.3K	79	€9.8B
Goods Receipts to PO & Maintain Purchase Order & Vendor Master Maintenance	5.1K	19	€1.3B
Goods Receipts to PO & Process Vendor Invoices	31.5K	44	€7.4B
Maintain Billing Documents & Maintain Customer Master Data	156	5	€755K
PO Approval & Maintain Purchase Order			
Process Customer Invoices & Maintain Customer Master Data			
Processing & Maintain Customer Master Data			

Process with the most critical exposures

 **User prompt**

Can you help me understand the volume of tickets our help desk handled over the past 7 months?

 **AI response**

Here's the monthly distribution of help desk tickets over the last 7 months, along with key takeaways:

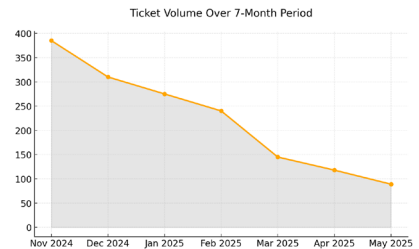
Key insights

Total volume: 1,562 tickets logged across the 7-month period

Peak activity: November 2024 saw the highest ticket volume, with 385 tickets submitted

Lowest activity: April 2025 had the fewest tickets, at just 118

Trend: Overall ticket volume has declined since November, with slight fluctuations in early 2025



Recommendation

The spike in November may be related to year-end processes, system rollouts, or policy changes. Consider increasing staffing levels or extending support hours during Q4 to ensure adequate coverage during this high-demand period.

The screenshot shows a software interface with a sidebar on the left and a main content area. The main content area is titled 'Exposures' and contains a summary of 40 exposures with a total amount of €37.8B and 275.3K alerts. A 'Co-pilot' chat window is overlaid on the right side of the interface, displaying the AI response text.

Vendor with the most alerts



User prompt

For which vendor are we getting the most alerts?



AI response

Based on current data, here's a key finding from the vendor analysis:

C.E.B. New York gets the most alerts at 3,028, representing over \$7.76 million in total financial exposure.

While the average dollar amount per alert is relatively low (approx. \$2,562), the volume of alerts is unusually high, which could indicate broader systemic or recurring issues.

Suggested next step: I recommend a deep-dive analysis into C.E.B. New York's exposure profile to understand the root cause of the alert volume, whether it's tied to process weaknesses, compliance gaps, or repeated anomalies that require attention. Would you like me to perform that analysis?

The screenshot shows a software interface with a 'Co-pilot' chat window. The chat window contains the following text:

Co-pilot

For which vendor are we getting the most alerts?

Highest Risk Vendor

Based on current data, here's a key finding from the vendor analysis:

- C.E.B. New York gets the most alerts at 3,028, representing over \$7.76 million in total financial exposure.
- While the average dollar amount per alert is relatively low (approx. \$2,562), the volume of alerts is unusually high, which could indicate broader systemic or recurring issues.

• Suggested next step: I recommend a deep-dive analysis into C.E.B. New York's exposure profile to understand the root cause of the alert volume, whether it's tied to process weaknesses, compliance gaps, or repeated anomalies that require attention. Would you like me to perform that analysis?

For which vendor are we getting the most alerts?

The background dashboard shows 'Exposures' with a summary of 40 total alerts (33 High, 6 Medium, 1 Low) and a total exposure amount of €37.8B out of €48B. It also displays a table of exposure items with columns for 'Total Alerts', 'Related Users', and 'Total Exposure'.

The significance of an alert

User prompt

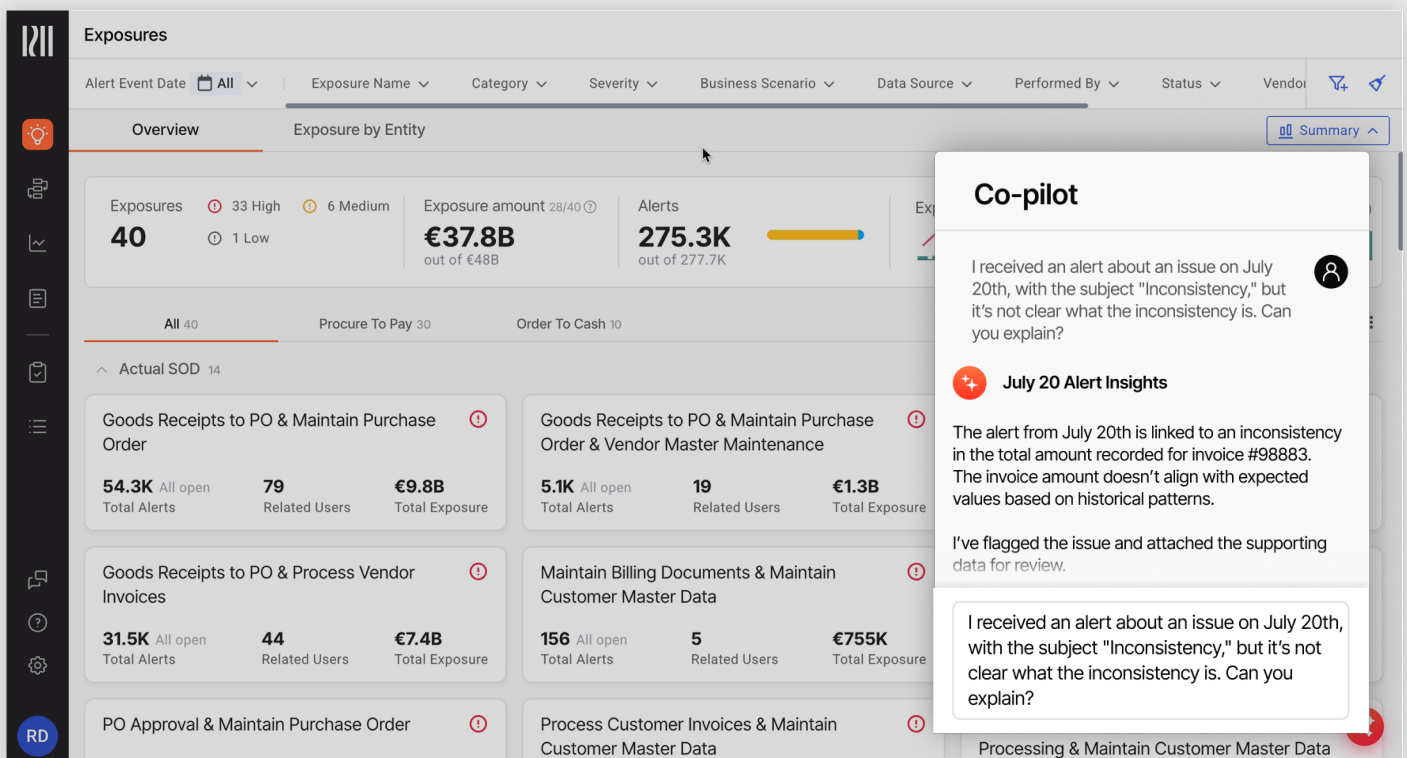
I received an alert about an issue on July 20th, with the subject "Inconsistency," but it's not clear what the inconsistency is. Can you explain?

AI response

The alert from July 20th is linked to an inconsistency in the total amount recorded for invoice #98883.

The invoice amount doesn't align with expected values based on historical patterns. I've flagged the issue and attached the supporting data for review.

[↓ July 20 supporting data](#)



The screenshot shows a software interface with a sidebar on the left and a main content area. The main content area is titled 'Exposures' and has a navigation bar with filters for Alert Event Date, Exposure Name, Category, Severity, Business Scenario, Data Source, Performed By, Status, and Vendor. Below the navigation bar, there are two tabs: 'Overview' and 'Exposure by Entity'. The 'Overview' tab is active and shows a summary of exposures and alerts. The summary includes: Exposures: 40 (33 High, 6 Medium, 1 Low); Exposure amount: €37.8B (out of €48B); Alerts: 275.3K (out of 277.7K). Below the summary, there are several cards representing different exposure categories, each with metrics for Total Alerts, Related Users, and Total Exposure. A 'Co-pilot' chat window is overlaid on the right side of the interface, containing a user prompt and an AI response.

Co-pilot

I received an alert about an issue on July 20th, with the subject "Inconsistency," but it's not clear what the inconsistency is. Can you explain?

July 20 Alert Insights

The alert from July 20th is linked to an inconsistency in the total amount recorded for invoice #98883. The invoice amount doesn't align with expected values based on historical patterns.

I've flagged the issue and attached the supporting data for review.

I received an alert about an issue on July 20th, with the subject "Inconsistency," but it's not clear what the inconsistency is. Can you explain?

Trigger behind a duplicate payment alert



User prompt

I received an alert titled "Duplicate Payment Detected," can you tell me what triggered it?



AI response

This alert was triggered by two identical payments made to WestBridge Supplies, for invoice #3421, each for \$18,750, processed within a one-day window.

I've highlighted both transactions and included supporting details for your review.

[↓ WestBridge Supplies duplicate payment details](#)

The screenshot shows the Datricks 'Exposures' dashboard. At the top, there are filters for Alert Event Date, Exposure Name, Category, Severity, Business Scenario, Data Source, Performed By, Status, and Vendor. The main view is 'Overview' with a sub-tab 'Exposure by Entity'. A summary card shows 40 total exposures (33 High, 6 Medium, 1 Low) with a total exposure amount of €37.8B out of €48B. Alerts are shown as 275.3K out of 277.7K. Below this, there are tabs for 'All 40', 'Procure To Pay 30', and 'Order To Cash 10'. A grid of exposure categories is displayed, including 'Goods Receipts to PO & Maintain Purchase Order', 'Goods Receipts to PO & Maintain Purchase Order & Vendor Master Maintenance', 'Goods Receipts to PO & Process Vendor Invoices', 'Maintain Billing Documents & Maintain Customer Master Data', and 'PO Approval & Maintain Purchase Order'. A 'Co-pilot' chat window is overlaid on the right, containing the user's prompt, the AI's response, and a link to 'WestBridge Supplies duplicate payment details'. The chat window also includes a 'Duplicate Payment Insights' section with the same AI response text.

Conclusion

In an era of growing data complexity and financial exposure, finance and internal audit teams need more than traditional tools.

They need real-time clarity and control over Financial Integrity.

This is where GenAI comes in.

With the power to automatically detect, clearly explain, intuitively guide, and act without being prompted, it transforms operations from manual to autonomous and from reactive to proactive, predictive, and corrective.

The future of finance and internal audit is powered by GenAI – intelligent, always-on, and built for Financial Integrity.



About Datricks

The Datricks Financial Integrity Platform transforms how finance and internal audit operate. At its core is a GenAI-powered intelligence layer that works 24/7 to protect and elevate your organization's Financial Integrity. It continuously and autonomously discovers, correlates, guides, and delivers deep, precision insights in real time.

By asking questions in simple natural language, and sometimes before you even ask, it provides instant answers, with data-led intelligence on anomalies, exposures, and correlations. This way you can prevent the damage of exposures resulting from errors, non-compliance, and fraud.

Datricks shifts finance from manual and reactive to AI-driven, autonomous operations with complete, real-time control that accelerates audit readiness, enhances governance, and drives smarter, faster decision-making across the enterprise.

To learn more, go to datricks.com

Get a demo

