konaAI

Leading Trends in Anti-Fraud Technology and Innovation

ACFE New York Chapter

October 20, 2023

Copyright © 2022 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

About the speaker: Vincent Walden, CFE, CPA



New York
vwalden@konaai.com

konaAI

- CEO of Kona AI
- 2022 “CFE of the Year,” awarded by the ACFE
- Passionate about forensic data analytics and building leading, AI-driven compliance technology and anti-fraud solutions
- Former Managing Director, Alvarez & Marsal (2019–May 2022)
- Former Partner, EY (2011–2019)
- Adjunct Professor at Fordham Law School, teaching compliance innovation
- Columnist for Fraud Magazine, writing on innovation in anti-fraud
- Co-author of the COSO/ACFE Fraud Risk Management Guide (2016 & 2023)
- Past president of the ACFE Education & Research Foundation

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Topics

- Forensic data analytics trends and regulatory drivers
- Aligning to COSO’s five fraud risk management principles
- The better the data, the better the insights
- Machine learning & AI primer
- Technology example
- Chatbots and the future of data analytics
- Audience questions and discussion



Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

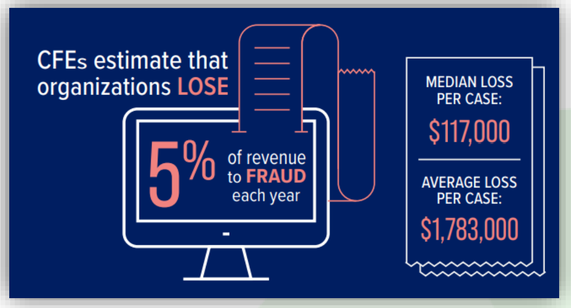
Trends and key innovations

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

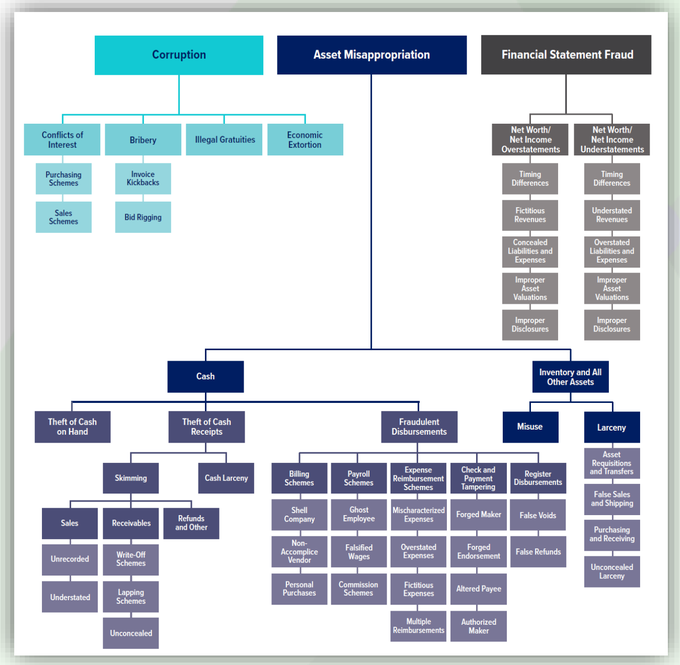
Key trends and statistics

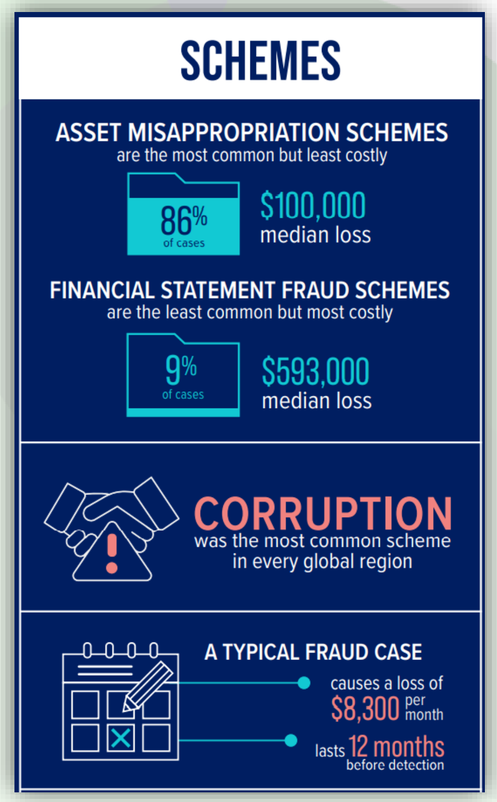
Trends & Innovations To Watch:

- Data visualization is here to stay
- Risk scoring is a must (reduce false positives)
- The better the data sources, the better the fraud risk questions
- The better the questions, the better the results & ROI
- No case management = no machine learning
- Machine learning is not that hard, but it does take time
- Generative AI and Chatbots will indeed change how its done
- Don’t worry, the human is not going away









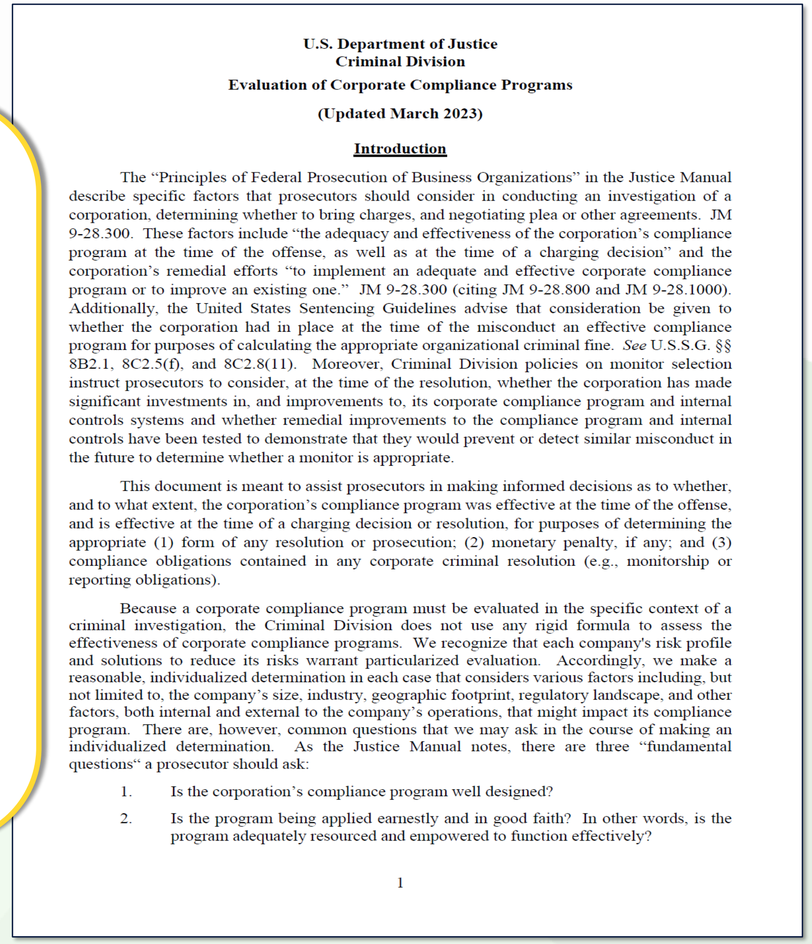
Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

The U.S. Department of Justice has an expectation of compliance monitoring after the contract is signed with the third party!

"Does the company engage in risk management of third parties throughout the lifespan of the relationship, or primarily during the onboarding process?"

"Do compliance and control personnel have sufficient direct or indirect access to relevant sources of data to allow for timely and effective monitoring and/or testing of policies, controls and transactions?"

"Do any impediments exist that limit access to relevant sources of data and, if so, what is the company doing to address the impediments?"



U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

1

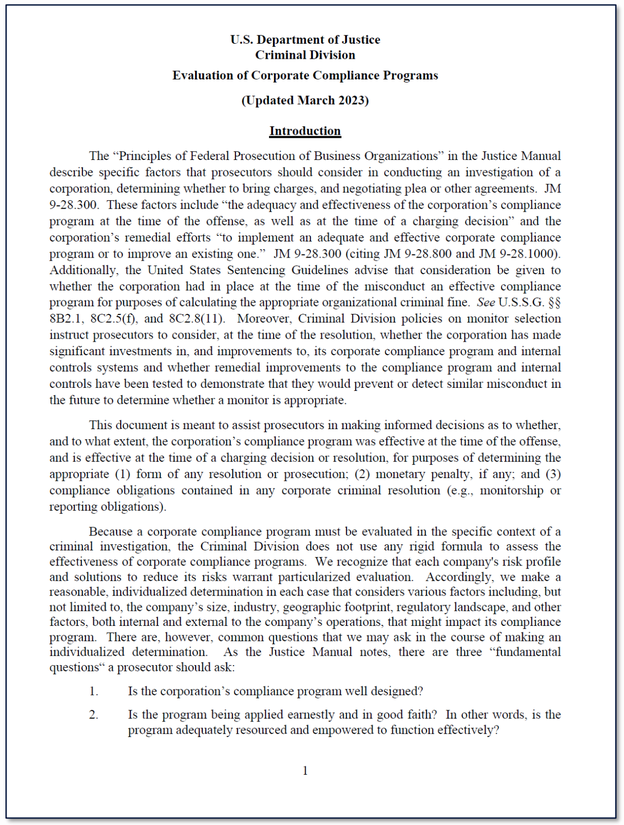
Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Aligning to the COSO / ACFE Fraud Risk Management Guide

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

Putting things in context – what is best practice guidance on anti-fraud?

DOJ: Evaluation of Corporate Compliance Programs



U.S. Department of Justice
Criminal Division

Evaluation of Corporate Compliance Programs

(Updated March 2023)

Introduction

The "Principles of Federal Prosecution of Business Organizations" in the Justice Manual describe specific factors that prosecutors should consider in conducting an investigation of a corporation, determining whether to bring charges, and negotiating plea or other agreements. JM 9-28.300. These factors include "the adequacy and effectiveness of the corporation's compliance program at the time of the offense, as well as at the time of a charging decision" and the corporation's remedial efforts "to implement an adequate and effective corporate compliance program or to improve an existing one." JM 9-28.300 (citing JM 9-28.800 and JM 9-28.1000). Additionally, the United States Sentencing Guidelines advise that consideration be given to whether the corporation had in place at the time of the misconduct an effective compliance program for purposes of calculating the appropriate organizational criminal fine. *See* U.S.S.G. §§ 8B2.1, 8C2.5(f), and 8C2.8(11). Moreover, Criminal Division policies on monitor selection instruct prosecutors to consider, at the time of the resolution, whether the corporation has made significant investments in, and improvements to, its corporate compliance program and internal controls systems and whether remedial improvements to the compliance program and internal controls have been tested to demonstrate that they would prevent or detect similar misconduct in the future to determine whether a monitor is appropriate.

This document is meant to assist prosecutors in making informed decisions as to whether, and to what extent, the corporation's compliance program was effective at the time of the offense, and is effective at the time of a charging decision or resolution, for purposes of determining the appropriate (1) form of any resolution or prosecution; (2) monetary penalty, if any; and (3) compliance obligations contained in any corporate criminal resolution (e.g., monitorship or reporting obligations).

Because a corporate compliance program must be evaluated in the specific context of a criminal investigation, the Criminal Division does not use any rigid formula to assess the effectiveness of corporate compliance programs. We recognize that each company's risk profile and solutions to reduce its risks warrant particularized evaluation. Accordingly, we make a reasonable, individualized determination in each case that considers various factors including, but not limited to, the company's size, industry, geographic footprint, regulatory landscape, and other factors, both internal and external to the company's operations, that might impact its compliance program. There are, however, common questions that we may ask in the course of making an individualized determination. As the Justice Manual notes, there are three "fundamental questions" a prosecutor should ask:

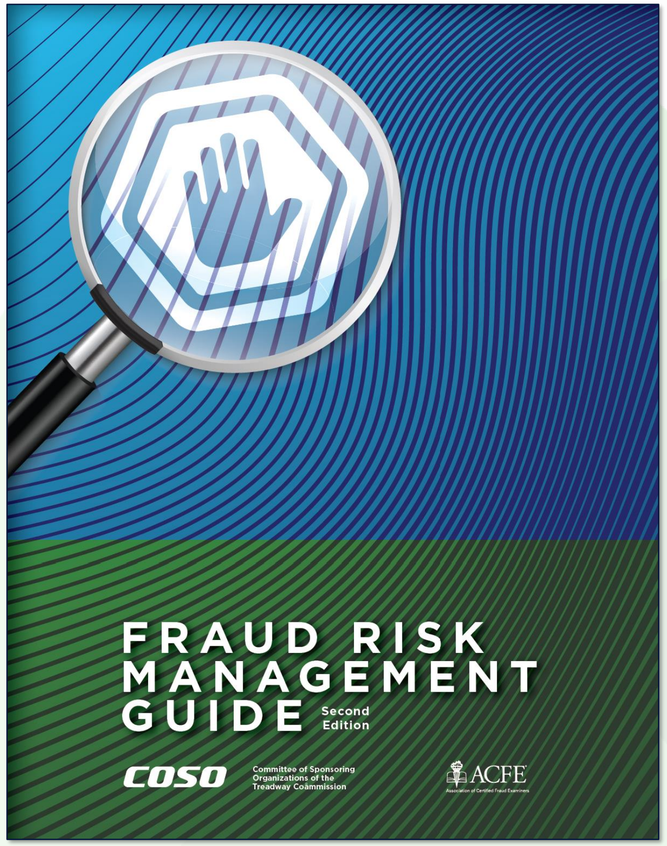
1. Is the corporation's compliance program well designed?
2. Is the program being applied earnestly and in good faith? In other words, is the program adequately resourced and empowered to function effectively?

1

- Written by attorneys for DOJ attorneys/prosecutors
- Risk assessment
- Policy & procedures
- Training & communications
- Confidential reporting & investigative process
- Third-party risk management
- Compliance program governance & effectiveness
- Use of data analytics

March 2023

COSO/ACFE: Fraud Risk Management Guide



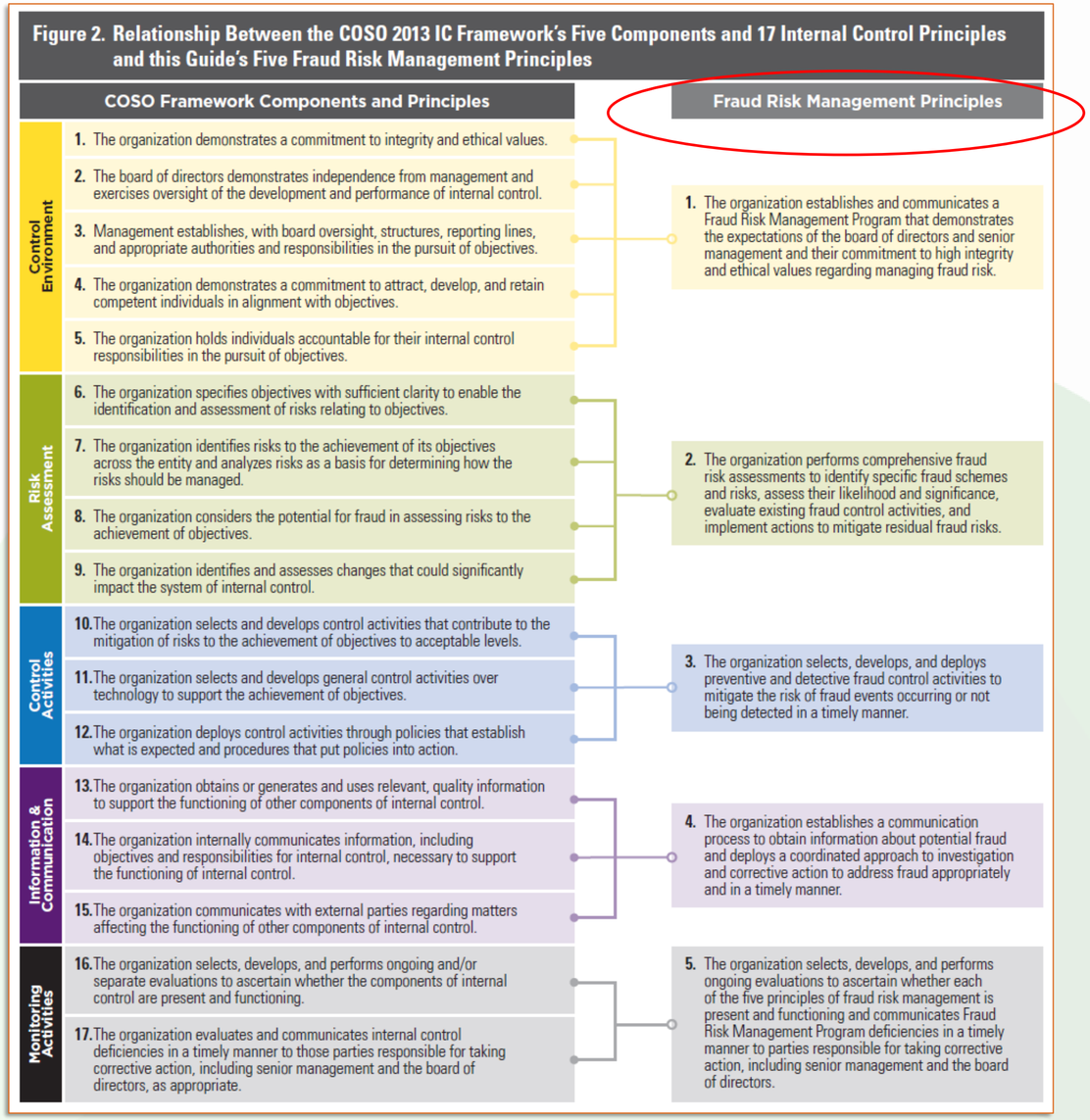
- Written by accountants & anti-fraud professionals
- Control environment
- Risk assessment
- Control activities
- Information & communication
- Continuous monitoring activities
- Use of data analytics

May 2023

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Linkage with COSO's Internal Controls Framework to the Five FRM Principles

- Start with the 17 COSO Principles of internal controls (SOX)
- Maps to the five FRM Principles
- Aligns well with the use of data analytics



Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Principle 1: Fraud Risk Governance

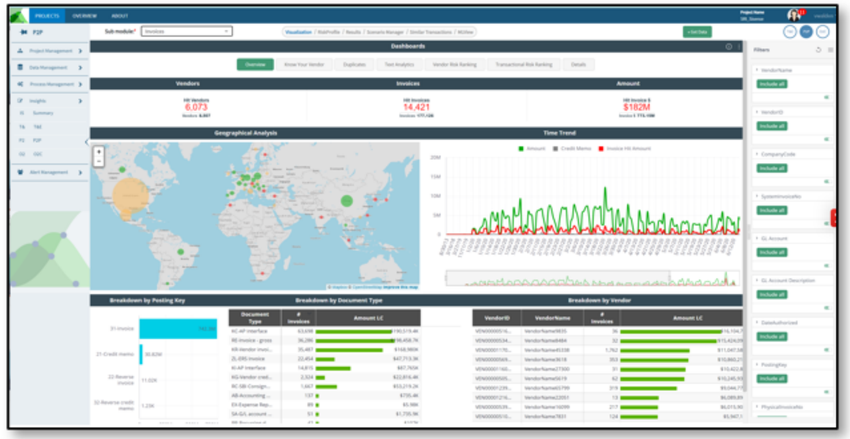
COSO 2013 Framework Principles → **Fraud Risk Management Principles** → **Analytic Considerations**

Control environment

1. The organization demonstrates a commitment to integrity and ethical values
2. The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
3. Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
4. The organization demonstrates a commitment to attract, develop and retain competent individuals in alignment with objectives.
5. The organization holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

1. The organization establishes and communicates a fraud risk management program that demonstrates the expectations of the board of directors and senior management and their commitment to high integrity and ethical values regarding managing fraud risk.

- Executive reporting
- Interactive dashboards
- Targeted analysis around metrics, compliance, and ratios

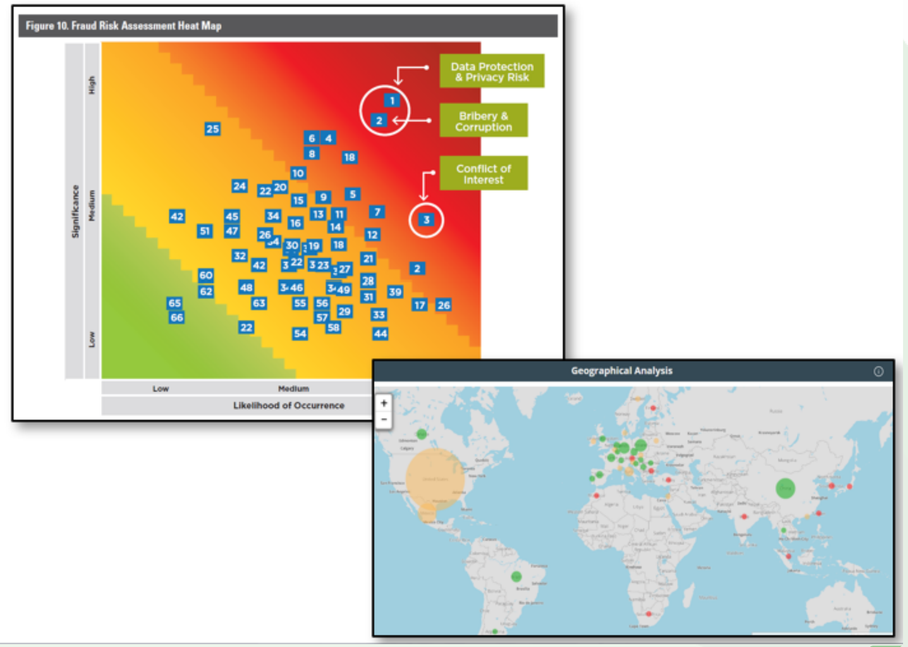


Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Principle 2: Fraud Risk Assessment

Risk assessment

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
6. The organization specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**2. The organization performs comprehensive fraud risk assessments to identify specific fraud schemes and risks, assess their likelihood and significance, evaluate existing fraud control activities, and implement actions to mitigate residual fraud risks.**	▸ Surveys and heat maps ▸ Media scans and external sources such as industry news ▸ Complaints database
7. The organization identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
8. The organization considers the potential for fraud in assessing risks to the achievement of objectives.		
9. The organization identifies and assesses changes that could significantly impact the system of internal control.		

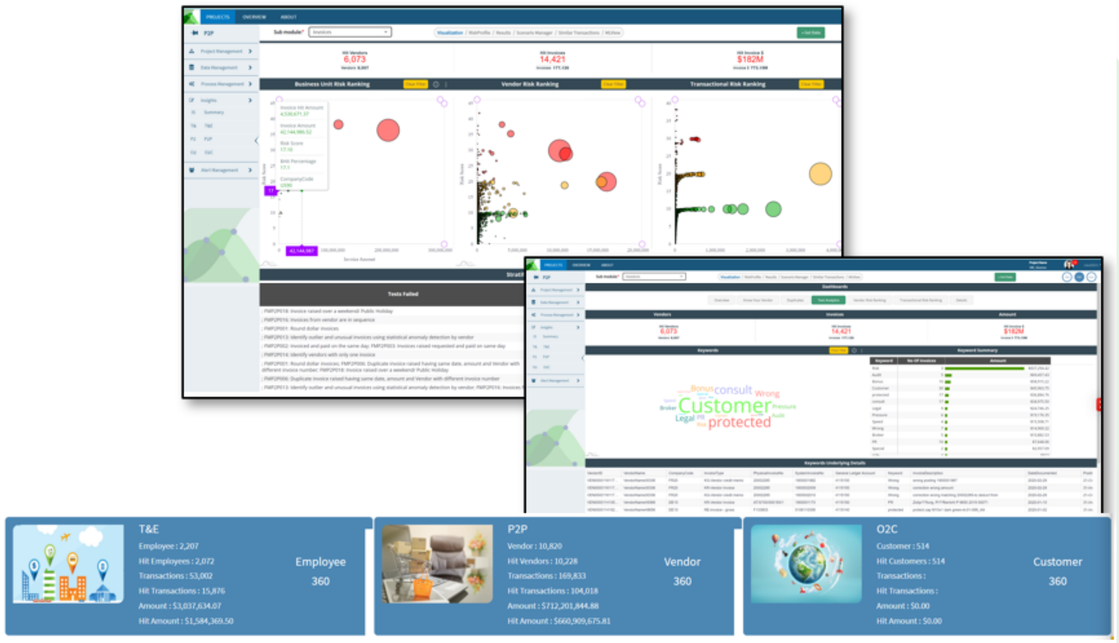


Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Principle 3: Fraud Control Activities

Control activities

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
10. The organization selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. 11. The organization selects and develops general control activities over technology to support the achievement of objectives. 12. The organization deploys control activities through policies that establish what is expected and procedures that put policies into action.	**3. The organization selects, develops, and deploys preventive and detective fraud control activities to mitigate the risk of fraud events occurring or not being detected in a timely manner.**	▸ Anti-bribery ▸ Sanctions compliance ▸ ESG ▸ P2P, O2C, T&E, CRM analysis ▸ Focus on vendors, customers & employees

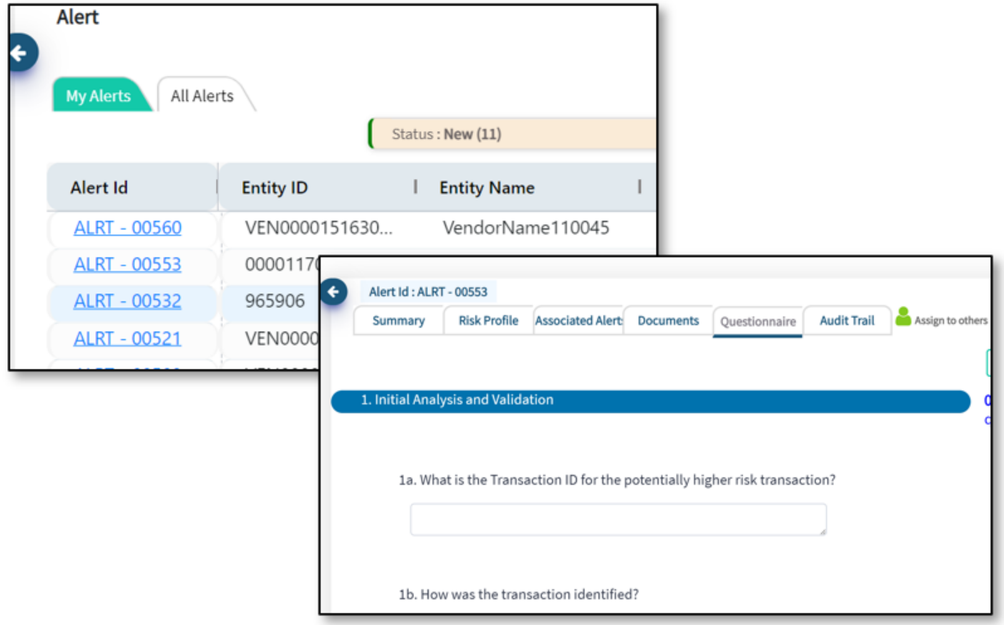


Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Principle 4: Incident Reporting, Investigation and Response

Information and communication

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
13. The organization obtains or generates and uses relevant quality information to support the functioning of other components of internal control. 14. The organization internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. 15. The organization communicates with external parties regarding matters affecting the functioning of other components of internal control.	**4. The organization establishes a communication process to obtain information about potential fraud and deploys a coordinated approach to investigation and corrective action to address fraud appropriately and in a timely manner.**	▶ Case management ▶ Escalation and triage ▶ Review workflow management

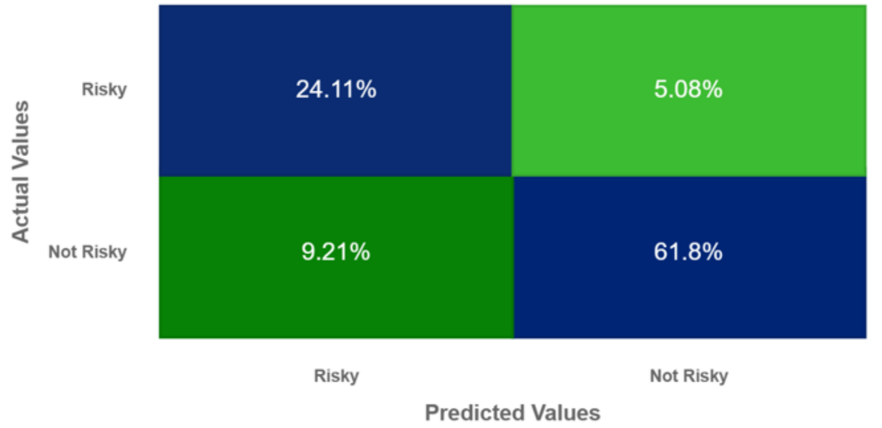


Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Principal 5: Monitoring Activities

Monitoring activities

COSO 2013 Framework Principles	Fraud Risk Management Principles	Analytic Considerations
16. The organization selects, develops and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. 17. The organization evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate	**5. The organization selects, develops, and performs ongoing evaluations to ascertain whether each of the five principles of fraud risk management is present and functioning and communicates fraud risk management program deficiencies in a timely manner to parties responsible for taking corrective action, including senior management and the board of directors.**	▸ Investigative procedures ▸ Continuous monitoring ▸ Continuous improvement ▸ Coordinates across the business and with other risk factors



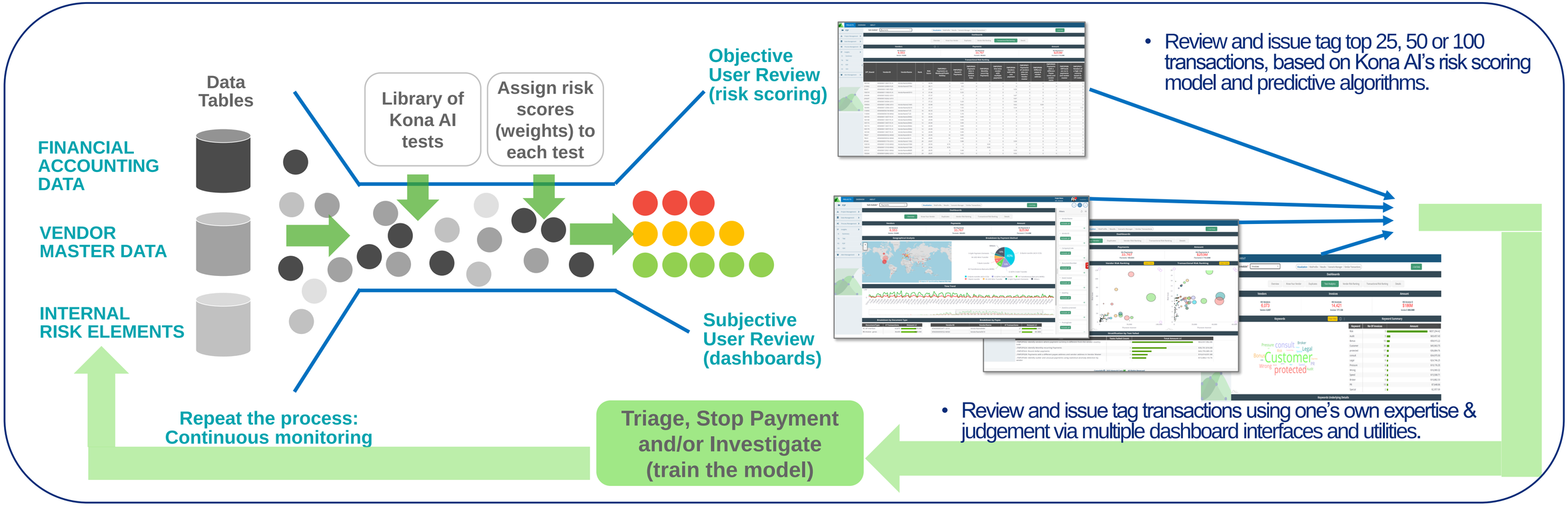
Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

The better the data, the better the insights

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

The better the data, the better the insights and ROI

Forensic Data Analytics Workflow





Vendor 360



Employee 360

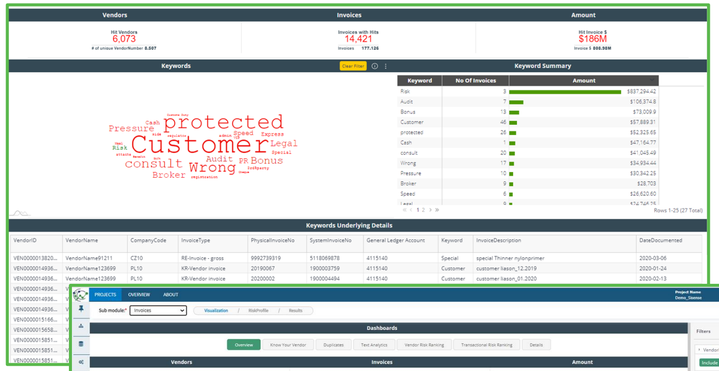


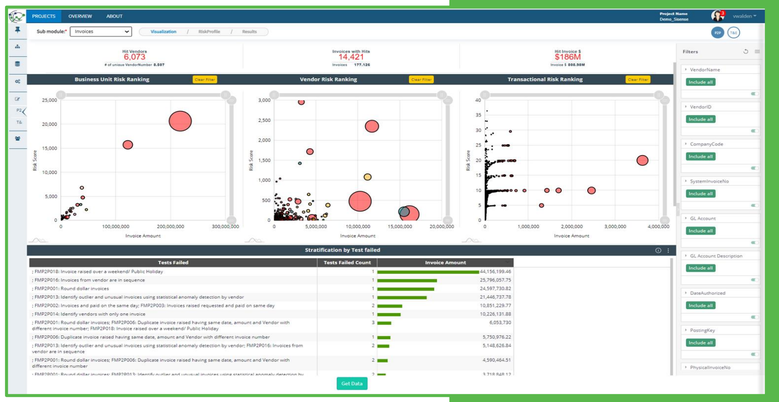
Customer 360

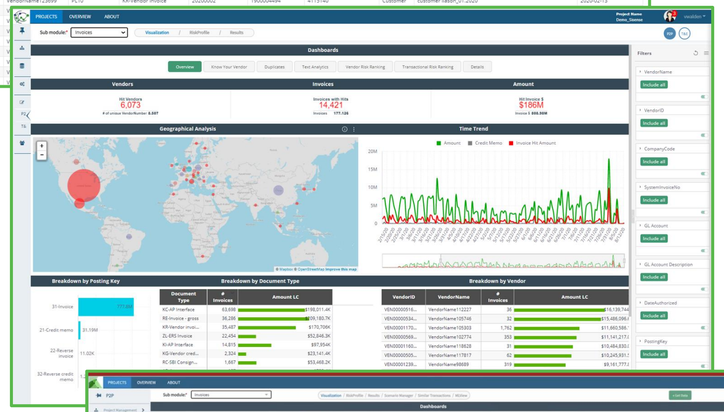
Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

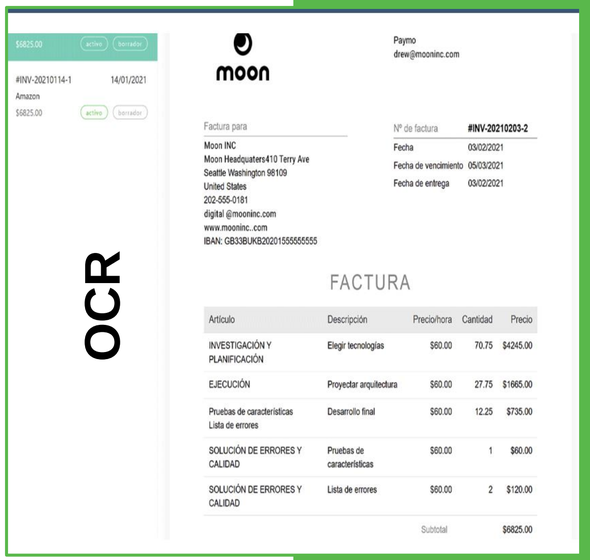
Think eDiscovery tools, but for structured data

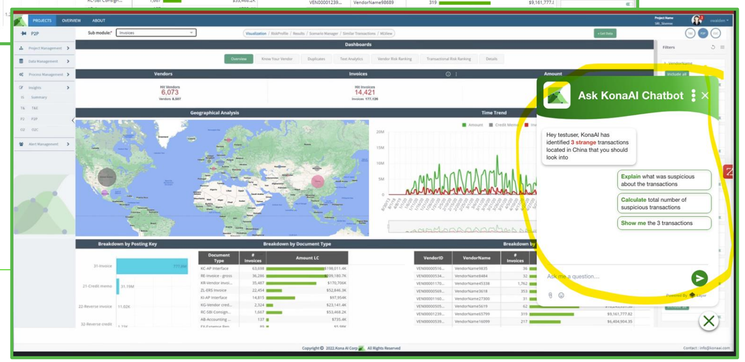
- User friendly dashboards (e.g., Tableau/PowerBI)
- End user training in about 1 – 2 hours.
- Transaction risk scoring.
- OCR matching: Invoices/receipts to entries
- Advanced text mining.
- Machine learning (“more like this”).
- Advanced behavioral algorithms.
- Full case management, workflow and transaction tagging / issue coding.
- Multiple business processes to risk rank vendors, customers, or employees.
- Coming soon: Generative AI bot assistance in dashboard navigation, suggestions and review, simply “Ask KonaAI”.











Copyright © 2022 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

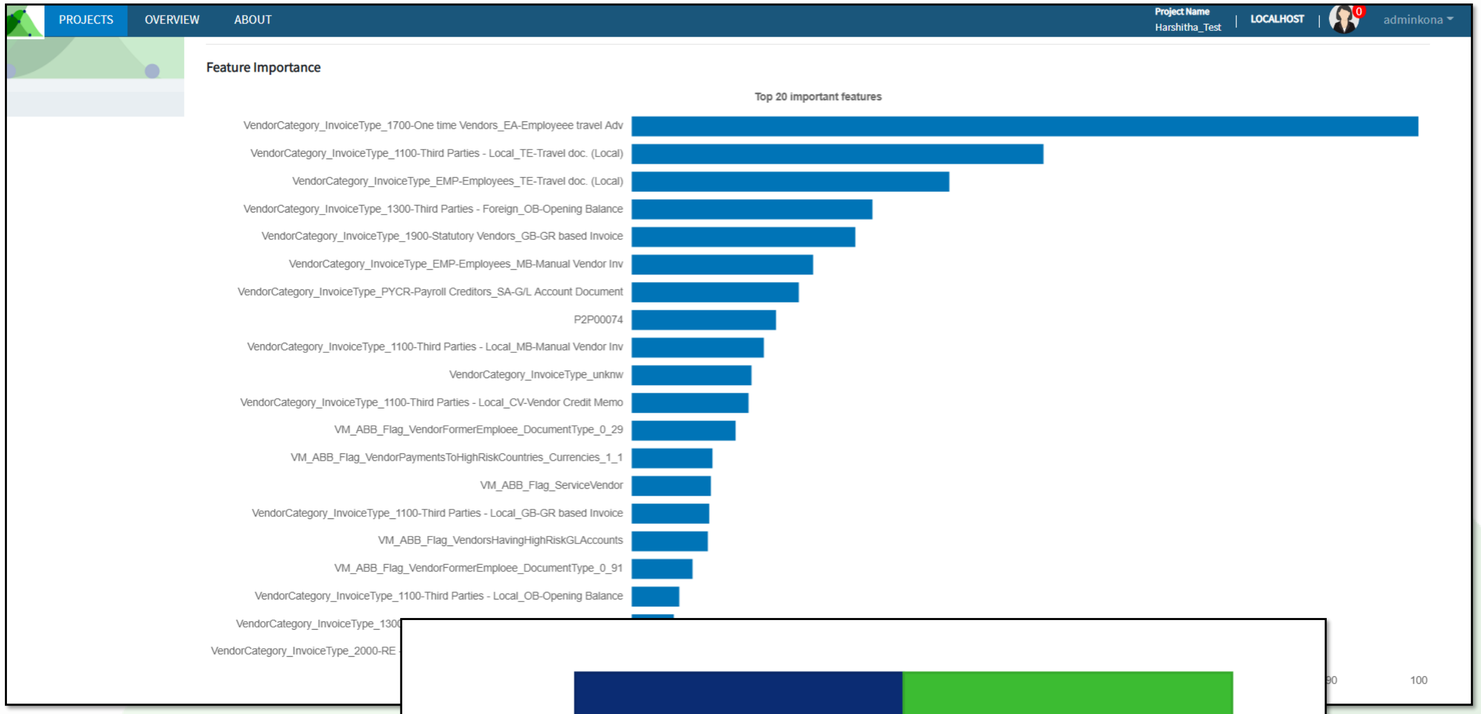
konaAI

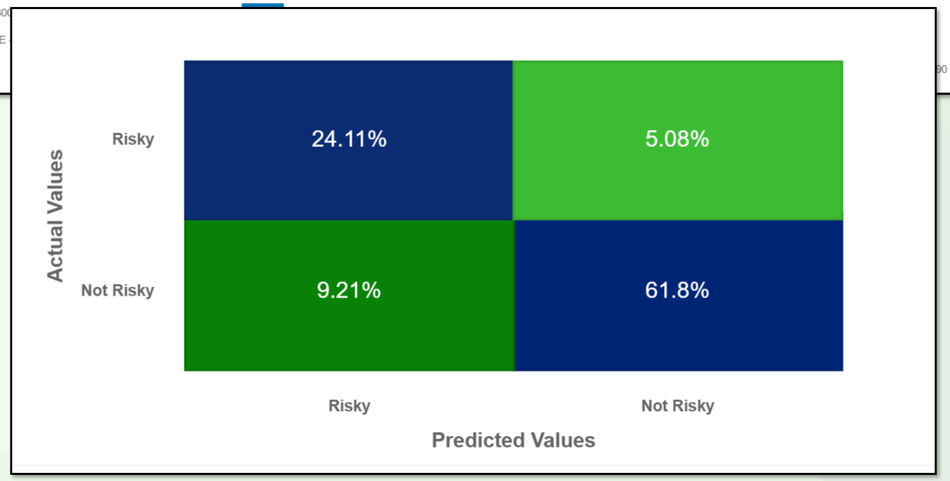
Machine leaning & AI primer

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

Machine learning concepts for forensic data analytics

- Review high-risk transactions
- Tag for relevancy
- Investigate and confirm
- Provide feedback into the model
- What's your F-1 score?





F1-score is the harmonic mean of the precision and recall.
A perfect model has an F-score of 1.

precision	Precision is the fraction of true positive examples among the examples that the model classified as positive. In other words, the number of true positives divided by the number of false positives plus true positives.
recall	Recall, also known as sensitivity, is the fraction of examples classified as positive, among the total number of positive examples. In other words, the number of true positives divided by the number of true positives plus false negatives.

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Profile of an improper (corrupt) payment: May/June 2023 FRAUD Magazine

RISK CATEGORY	SUB MODULE	DESCRIPTION	% HIT
Controls validation	Purchase Order	Vendors in POs not in the vendor master	8.69%
Corruption pattern	Purchase Order	Material description analytics using FCPA key-word list – English	3.12%
Statistical anomaly	Payments	Identify outlier and unusual payments using statistical anomaly detection by vendor	2.74%
Transaction anomaly	Payments	Identify monthly recurring payments	2.58%
Transaction anomaly	Invoices	Duplicate invoice raised having same date, amount and vendor with different invoice number	2.20%
Temporal	Invoices	Invoice raised over a weekend/public holiday	2.18%
Transaction anomaly	Invoices	Round dollar invoices	1.96%
Controls validation	Purchase Order	Vendor is missing from the purchase order	1.88%
Transaction anomaly	Purchase Order	Duplicate POs based on same vendor, material/ item within 0-5 days range	1.63%
Conflict of interest	Payments	Employees with same address but different names with payments	1.63%



INNOVATION UPDATE | Building your professional future

PROFILE OF AN IMPROPER (CORRUPT) PAYMENT

What are the telltale signs of an improper payment? Here we explore the leading research into what can be measured and observed to find common patterns and profiles around improper, and sometimes corrupt, payments.

If we were somehow able to see all of history's bribes, kickbacks, conflicts of interests, duplicative payments, fake vendors, restricted entities and anomalous transactions from multiple companies and/or multiple regulatory enforcement actions, what would be some of the common threads? What common keywords do people use to describe an improper payment?

I posed these and other questions to some of the data scientists on my team who worked on a research project with the Anheuser-Busch InBev Foundation and the MIT researchers at Integrity Distributed (InDi), a nonprofit anti-fraud and anti-corruption think tank. In this research, we looked at the predictive modeling improvements when companies collaborate to fight corruption — without having to share the underlying data. Within that model, we can also analyze what attributes (or variables) were driving that model in hopes of unlocking the profile of an improper or corrupt payment.

Here were a few of my other queries for the research team:

- What's the most common general ledger account an improper expense is booked to?
- What anti-fraud test is most common among the population of these known fraudulent transactions?
- Are manual payments the norm, or are they outliers? Are there occasions where manual payments are being abused for personal benefits?

COLUMNIST
VINCENT M. WALDEN, CFE, CPA
CEO KONA AI

Knowing whether a transaction is benign or indeed a high-risk or improper payment is an important distinction that often challenges prosecutors, lawyers and anti-fraud professionals like us. It takes time to gather evidence, review source documentation, run selected anti-fraud algorithms and analytics, and interview suspected individuals. If we could, with statistical confidence, quickly identify and remediate improper payments — perhaps even before they get paid out to a third party — we could not only save our organizations tremendous amounts of time and money, but also keep our organizations out of trouble with regulators.

Indeed, now more than ever, organizations using data analytics and collaborative initiatives such as InDi have an incentive to quickly and proactively identify and substantiate risks to determine if self-disclosure is necessary. That's because, in February, the U.S. Department of Justice announced a new standard of voluntary self-disclosure. Under the new standard, one of the factors of leniency hinges on a company's voluntary disclosure of misconduct to the U.S. Attorney's Office "within a reasonably prompt time after the company becoming aware of the misconduct, with the burden being on the company to demonstrate timeliness," potentially resulting in non-prosecution agreements and reduced fines. (See "United States Attorneys' Offices Voluntary Self-Disclosure Policy," justice.gov press release, tinyurl.com/kj4spfzx.)

What can be measured?

Roopak K. Prajapat is an advisor to the InDi team and Anheuser-Busch InBev's lead data scientist/global director on their BrewRIGHT compliance monitoring platform, which focuses on building predictive models to proactively identify, prevent and detect potentially improper payments using machine-learning algorithms. Prajapat says that with today's advances in machine learning and artificial intelligence (AI), the possibilities are quite exciting, especially when companies collaborate to fight corruption. Through guidance and work on the InDi project, which has (to date) processed over $75 billion in third-party vendor payments across nearly a dozen Fortune 500 companies, Prajapat is starting to garner some important insights about high-risk payments.

However, Prajapat cautions that the results are still evolving and not yet conclusive, as the models need to be further trained with better classifications (or tagging of improper payments). He also says that it's incumbent upon legal, compliance and anti-fraud professionals to diligently identify and document any vulnerabilities or weaknesses in the organization's processes that malicious actors could potentially exploit. By doing so, these professionals can provide

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Generative AI: Hey, ChatGPT, write me a presentation on FDA

Good morning/afternoon/evening, ladies and gentlemen. Today,
I would like to talk to you about an increasingly important field in
the world of data analysis and investigations: Forensic Data Analytics. In this digital age, where vast amounts of data are generated and stored, organizations are faced with numerous challenges in detecting and preventing fraud, mitigating risks, and ensuring compliance with regulations. Forensic Data Analytics provides a powerful solution to address these challenges by leveraging advanced analytical techniques and tools to uncover insights, identify patterns, and detect anomalies within large datasets.

So, what exactly is Forensic Data Analytics? It is the application of data analysis and investigative techniques to identify and investigate potential fraud, misconduct, or noncompliance within an organization. It involves the collection, analysis, and interpretation of data from various sources such as financial systems, transactional records, emails, and other digital footprints. By analyzing these datasets, forensic data analysts can uncover hidden patterns, unusual behaviors, and potential red flags that may indicate fraudulent activities.

Let's delve into some key aspects of Forensic Data Analytics:

1. Fraud Detection: Forensic Data Analytics plays a vital role in fraud detection and prevention. By analyzing large volumes of
   data, anomalies and irregularities can be identified, helping organizations to proactively detect potential fraudulent activities. Whether it's detecting fraudulent transactions, suspicious patterns in financial statements, or employee misconduct, forensic
   data analysis enables timely intervention to mitigate risks and minimize losses.
2. Risk Assessment and Compliance: Effective risk management and compliance are crucial for organizations to maintain their integrity and reputation. Forensic Data Analytics helps in identifying areas of vulnerability, assessing risks, and monitoring compliance with regulatory frameworks. By analyzing data related to internal controls, transactional activities, and operational processes, organizations can identify potential weaknesses and take appropriate measures to strengthen their systems.
3. Investigation and Evidence Gathering: In cases where fraud or misconduct is suspected, forensic data analysts play a crucial
   role in investigations. They utilize advanced data analysis techniques to identify relevant information, reconstruct events, and uncover evidence. This includes analyzing communication records, financial transactions, and other digital artifacts to build a comprehensive picture of the situation and support legal proceedings, if necessary.
4. Continuous Monitoring and Auditing: Forensic Data Analytics enables organizations to implement continuous monitoring and auditing processes. By leveraging automated data analysis tools and techniques, organizations can proactively monitor transactions, identify anomalies, and implement real-time fraud detection controls. This helps in minimizing the risk of fraud
   and ensuring compliance on an ongoing basis.
5. Data Visualization and Reporting: One of the key strengths of Forensic Data Analytics is its ability to transform complex datasets into meaningful visualizations and reports. By presenting data in a visually appealing and easy-to-understand manner, stakeholders can quickly grasp the insights and make informed decisions. Visual representations also aid in communicating findings and recommendations effectively to management, regulators, or legal authorities.

In conclusion, Forensic Data Analytics is a powerful tool for organizations to proactively detect, investigate,
and prevent fraud, misconduct, and noncompliance. By leveraging advanced analytical techniques, organizations can gain deeper insights from their data, identify patterns, and detect anomalies that may otherwise go unnoticed. This field continues to evolve as technology advances, and it is essential for organizations to stay abreast of the latest trends and tools to effectively combat fraud and ensure compliance. Thank you for your attention, and I am happy to address any questions or concerns you may have.

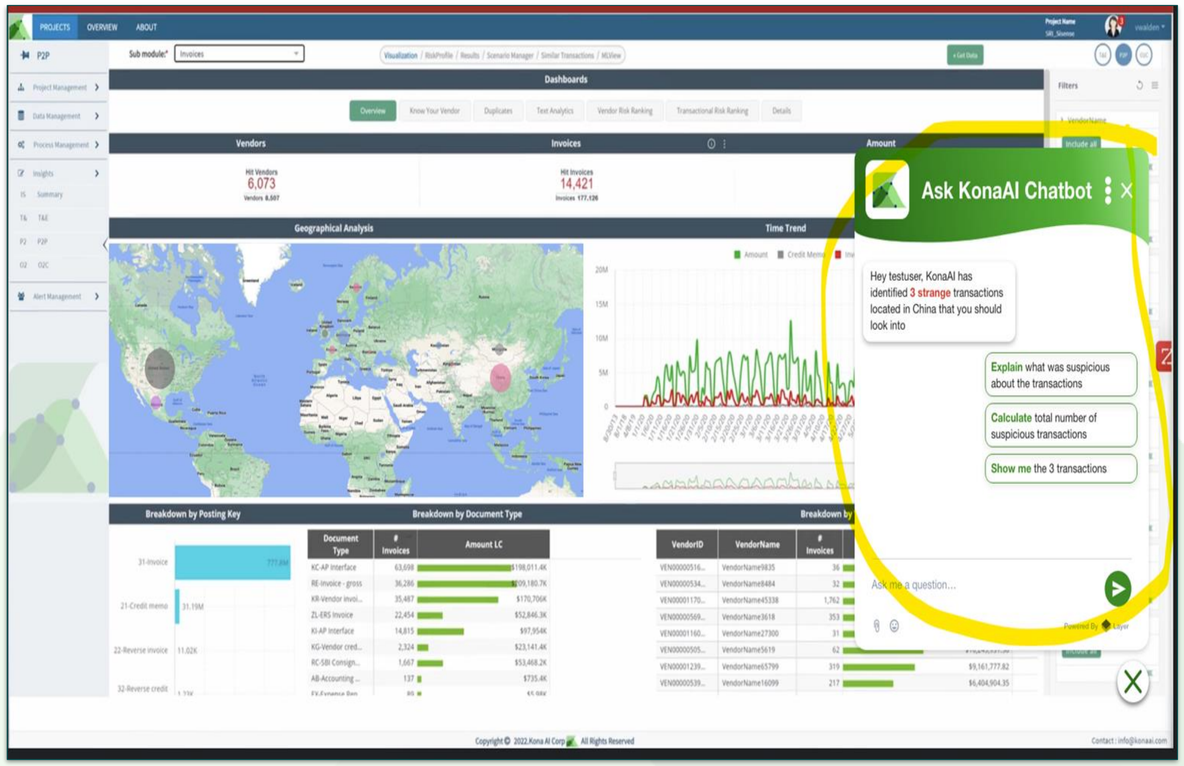
Example only from ChatGPT

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Generative AI: Pointing at your financial accounting data (securely)

- Show me my highest risk transactions (or vendors) for…
- Show me any invoice with the word “training” in the description, in Argentina, within the last 60 days.
- Find me similar transactions to <selected transaction>.
- Which employees are at risk for paying a bribe?
- What are my top 10 highest risk transactions? Or top 10 riskiest customers / vendors / employees?

Group
Payments (80)
Conflict Of Interest (7)
Transaction anamoly (27)
Seggregation of duty validation (10)
Vendor Process Manipulation (8)
Temporal (3)
Spend pattern (6)
Controls validation (7)
Unsupported Spend (1)
Keywords (1)
Price Manipulation (2)
Corruption pattern (6)
Policy Violation (1)
High Risk Country (1)



Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Sept./Oct. issue of FRAUD Magazine

- What is ChatGPT, what it is not
- Use case examples
- The dark side of Generative AI
- Unstructured and structured use cases (demo)

MIND BLOWING

HOW GENERATIVE AI CAN HELP IN FRAUD PREVENTION AND ANALYTICS

Understanding ChatGPT and similar generative AI tools is critical for fraud examiners seeking to leverage this emerging technology. Here we explore the risks and the extraordinary potential of this new phenomenon.

At the 34th *Annual ACFE Global Fraud Conference* in June, I gave a presentation, in two identical sessions, on ChatGPT and generative artificial intelligence (AI). Both sessions were standing-room-only with a combined attendance of over 1,600 in-person and online. Trust me, it wasn't me they crowded the conference room for — it was the topic. The presentation's popularity sent me a clear message: Fraud examiners are eager to learn about this exciting, emerging area of technological innovation.

So, for those who were unable to attend, I'd like to share the important takeaways in this column. Like many of my anti-fraud technology colleagues, I find myself immersed in a whirlwind of excitement surrounding generative AI and how it can impact fraud prevention and detection. The sheer potential of generative AI technologies has ignited a frenzy of curiosity and anticipation in all industries. The hype isn't unfounded. It stems from the transformative capabilities that generative AI vehicles like ChatGPT bring to the table. Let's examine what ChatGPT is, what it isn't, and how it will indeed transform how you look and interact with your data in the very near future.

What are ChatGPT and generative AI?

ChatGPT is an AI chatbot developed by OpenAI and released last November. (See openai.com.) "Chat" is a reference to it being a chatbot, and "GPT" stands for generative pre-trained transformer — a type of large language model (LLM). Think of an LLM not as an advanced law degree, but as a super-large body of content that's indexed for search and training of the model. In ChatGPT's case, the LLM consists of over 300 billion words, mostly scraped from the internet.

So then, what's this term "generative AI"? It's a type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data. ChatGPT is a popular form of generative AI, as are Google Bard and many other generative AI tools available online either for free or at a price.

So many use cases, but this one will blow your mind

ChatGPT is, essentially, a content creation, "ask me anything" type of tool. People use ChatGPT for first draft product descriptions, blog posts, social media posts, drafts of new business ideas or even drafting of entire articles. It also works well for language translation, conversational AI chatbots, writing code (even malware), policy writing, courses and educational content creation, help with your kid's homework, research assistance, customer support and even surveys. Have a look at what the free version of ChatGPT came up with when I asked it to write me a fraud risk management survey. (See Figure 1 above.)

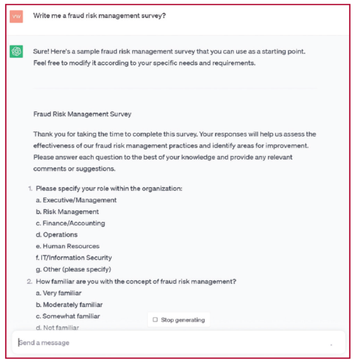


Figure 1 *Source: OpenAI*

Interestingly, you typically won't get the exact same answer twice to the same question, and I'm told that the paid version of ChatGPT produces better, or more, results than the free version.

All of these "unstructured" data use cases are cool and rather impressive. But being focused on innovation, I wanted to take it a step further. What happens if we point generative AI tools to a structured data source like accounting data? Could we use it to help us identify potentially improper, corrupt or fraudulent payments to vendors? Could it identify high-risk employees abusing travel-and-entertainment expenses, or high-risk customers or distributors via a company's sales transactions?

Instead of clicking around in your Tableau or PowerBI dashboard, could an AI chatbot do the navigation for you — seamlessly directing you to high-risk transactions, such as those listed in Figure 2 on page 57, and provide recommendations on where to go next?

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.

Technology demo

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

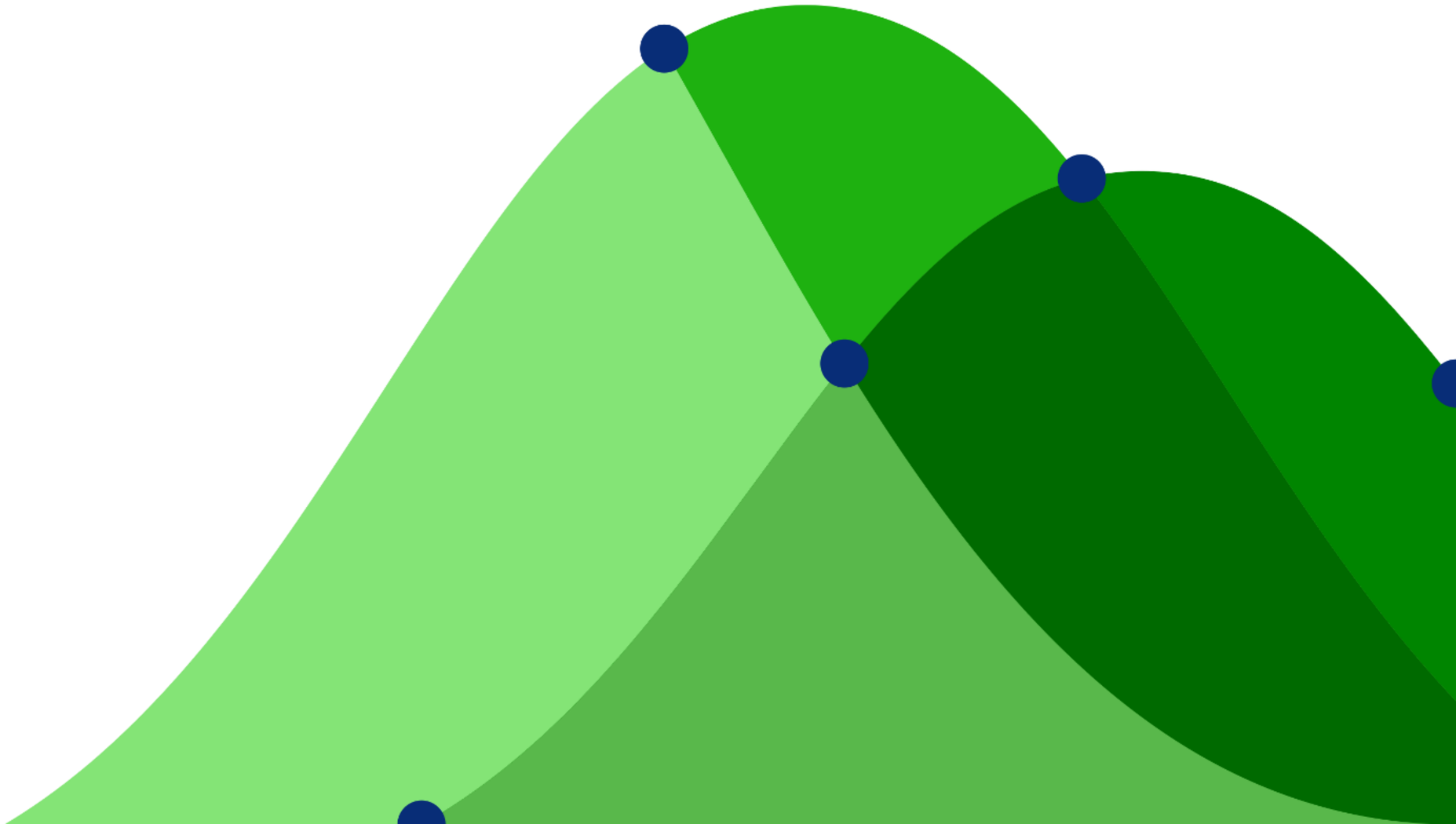
Questions & discussion

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners. Subject to NDA. CONFIDENTIAL.

konaAI

Thank you

Vincent Walden
+1-940-230-4648
vwalden@konaai.com



www.konaAI.com

Copyright © 2023 Kona Data Sciences. All rights reserved. Trademarks are the property of their respective owners.