HIDDEN IN PLAIN SIGHT:

FIGHTING FRAUD WITH DATA ANALYTICS

Let's connect!

BETHMARA KESSLER, CFE

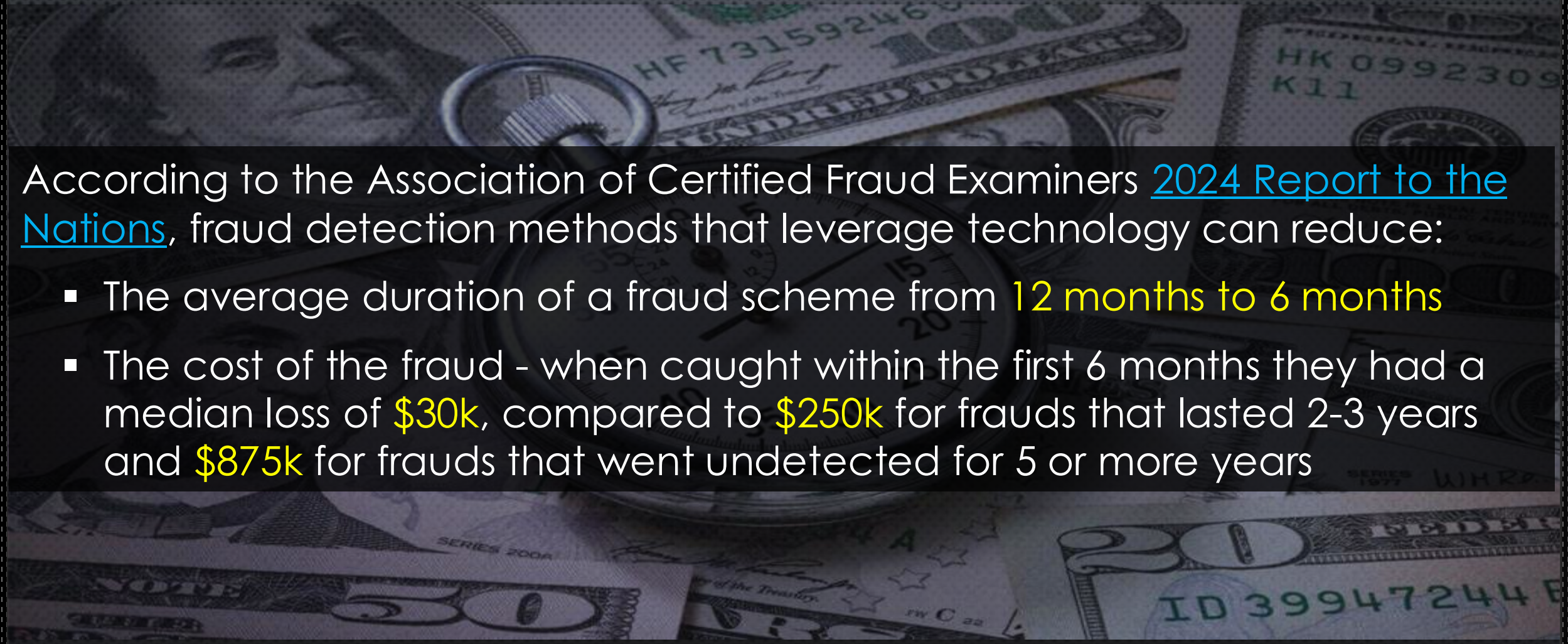
Agenda

- Benefits of leveraging data analytics for fraud detection
- Most common red flags of fraud that hide in the data
- Actionable steps to jumpstart or elevate your data driven fraud detection efforts

Data Analytics for Fraud Detection – The Benefits

- Many times, the evidence of fraud is hiding in plain sight - If we look for it, we can find it
- Fraudsters often leave breadcrumbs of their fraud or the concealment of their actions
- Using manual techniques to detect fraud can feel like looking for a needle in a haystack
- Effective fraud detection methods will make a fraudster think twice

Data Analytics for Fraud Detection – The Benefits



According to the Association of Certified Fraud Examiners 2024 Report to the Nations, fraud detection methods that leverage technology can reduce:

- The average duration of a fraud scheme from 12 months to 6 months
- The cost of the fraud - when caught within the first 6 months they had a median loss of $30k, compared to $250k for frauds that lasted 2-3 years and $875k for frauds that went undetected for 5 or more years

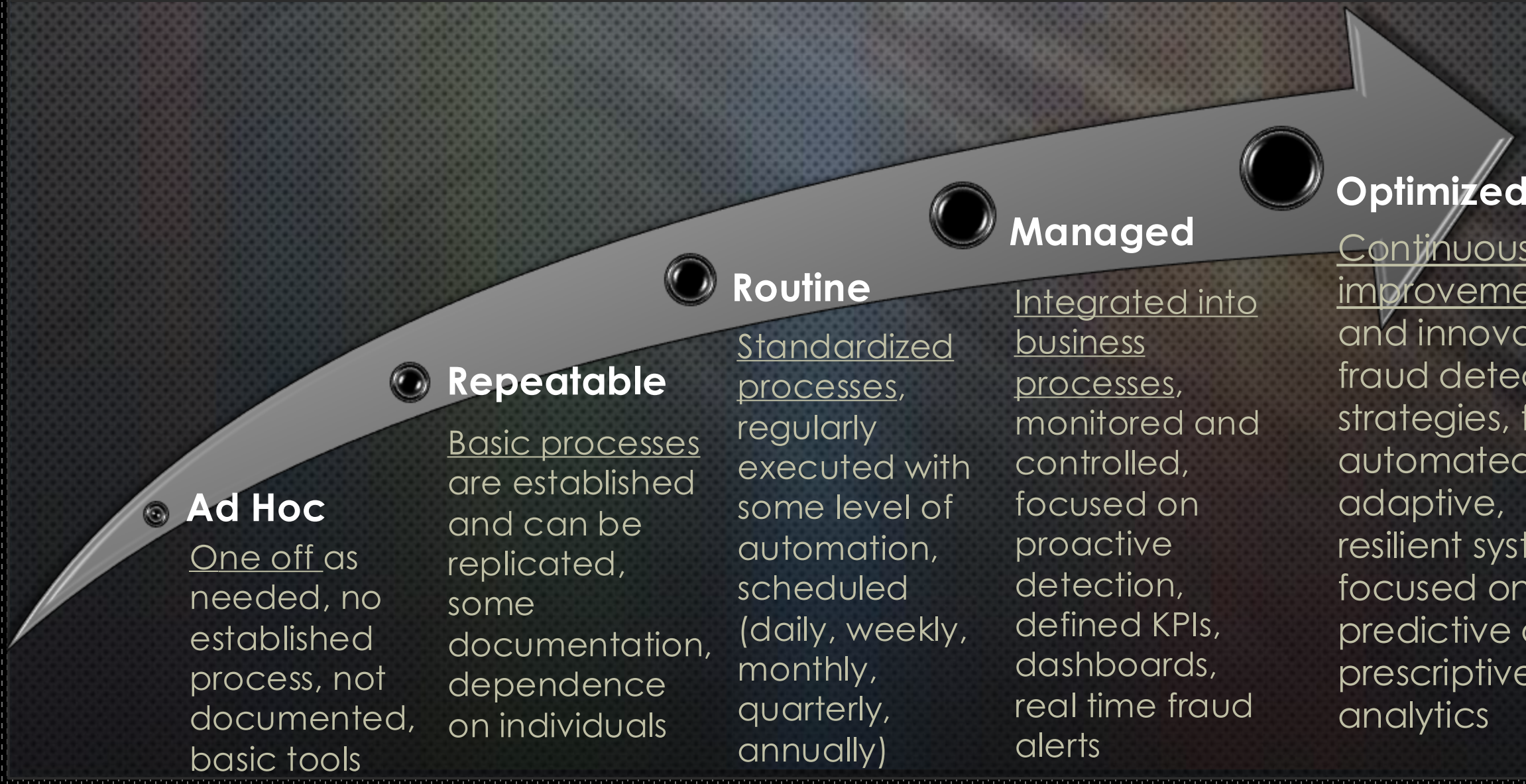
Data Analytics for Fraud Detection – The Benefits

- Improves Accuracy
- Enables Scalability
- Supports Strategic Decision Making
- Builds Resiliency
- Fosters Continuous Improvement
- Enhances Reputation and Trust

Data Analytics for Fraud Detection - Use Cases/Example

Descriptive	Diagnostic	Predictive	Prescriptive
What happened?	Why did it happen?	Based on what happened what is likely to happen next?	Using complex simulations, what is likely to happen in the future?
The credit card company claimed that a number of our customer orders are fraudulent and they charged us back - we analyzed all activity over 6 months and found ____ chargebacks totaling $_____	We isolated the ___ chargebacks and analyzed them. We found a spider web connecting IP addresses, physical addresses, and similar names from one initial bad customer to all fraudulent activity	We developed a fraud scoring model to predict new order activity likely tied to the fraud ring using the historical fraudulent data - we cancelled >__ highly suspicious orders before goods were shipped	We created complex model simulations to help understand how the fraud ring behaviors would likely evolve into new high impact fraudsters, enabling us to design actions to mitigate risk

Data Analytics for Fraud Detection – Maturity Model



Red Flags in the Data

- ☒ Unusual
- ☒ Illogical
- ☒ Inconsistent/Unexpected
- ☒ Frequent/infrequent
- ☒ Too large/too small

- ☒ Missing information
- ☒ Confusing information
- ☒ Duplicate information
- ☒ Generic information
- ☒ Key word usage

"One of these things is not like the other, one of these things just doesn't belong"
Sesame Street

Common Red Flags in the Data

- Round number transactions
- Transactional activity spikes near period end
- Top side/manual journal entries near period end
- "Off hours" activity
- Frequent adjustment activity
- Activity "just below" the threshold
- Missing info or unexpected changes to master data
- Vendors that are not typically business related
- Descriptions that are nonspecific, generic or jargon

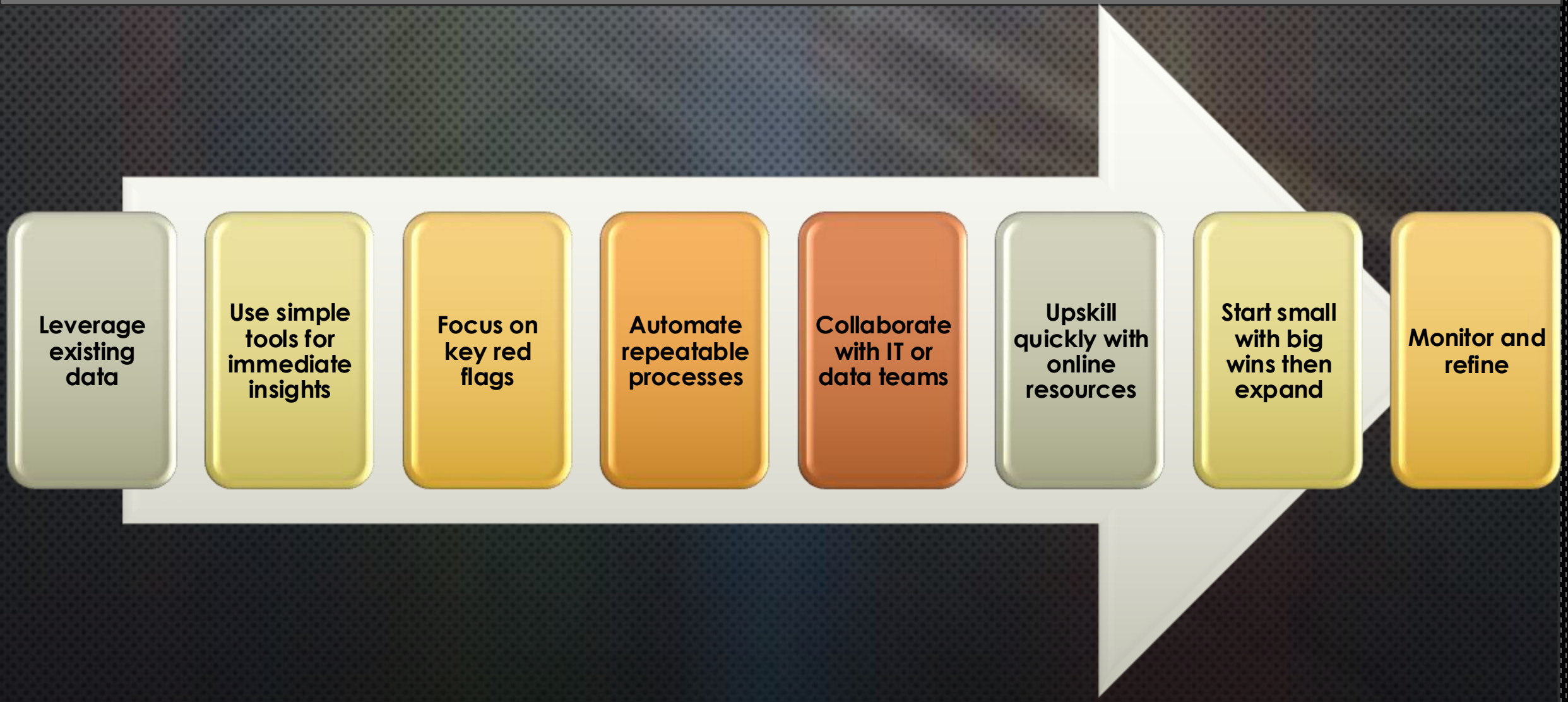
Finding Red Flags in the Data – Example Techniques

- Quantitative Analytics
- Trend or Pattern Analyses
- Ratio Analyses
- Textual or Sentiment Analyses
- Geospatial Analyses
- Velocity or Time Based Analyses
- Behavioral Analyses
- Relationship or Network Analyses

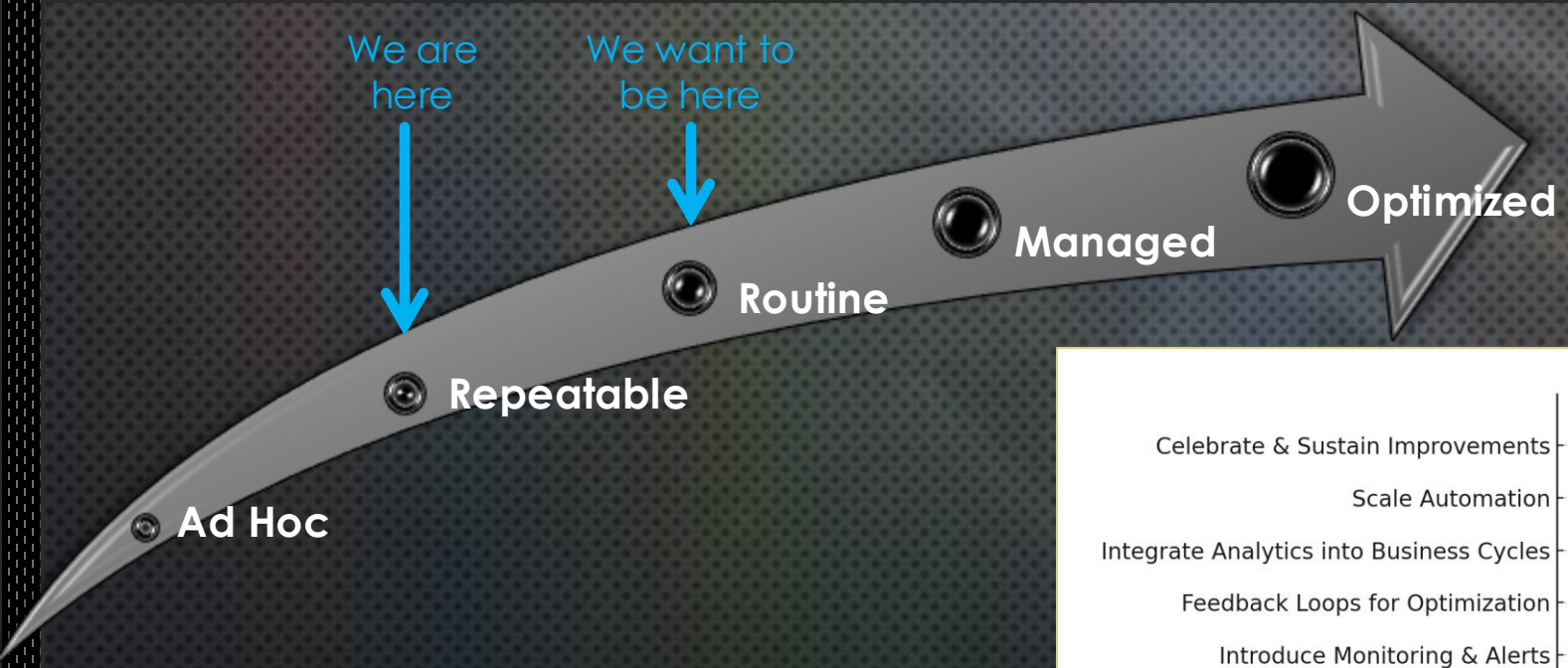
Actionable Steps – Getting Started

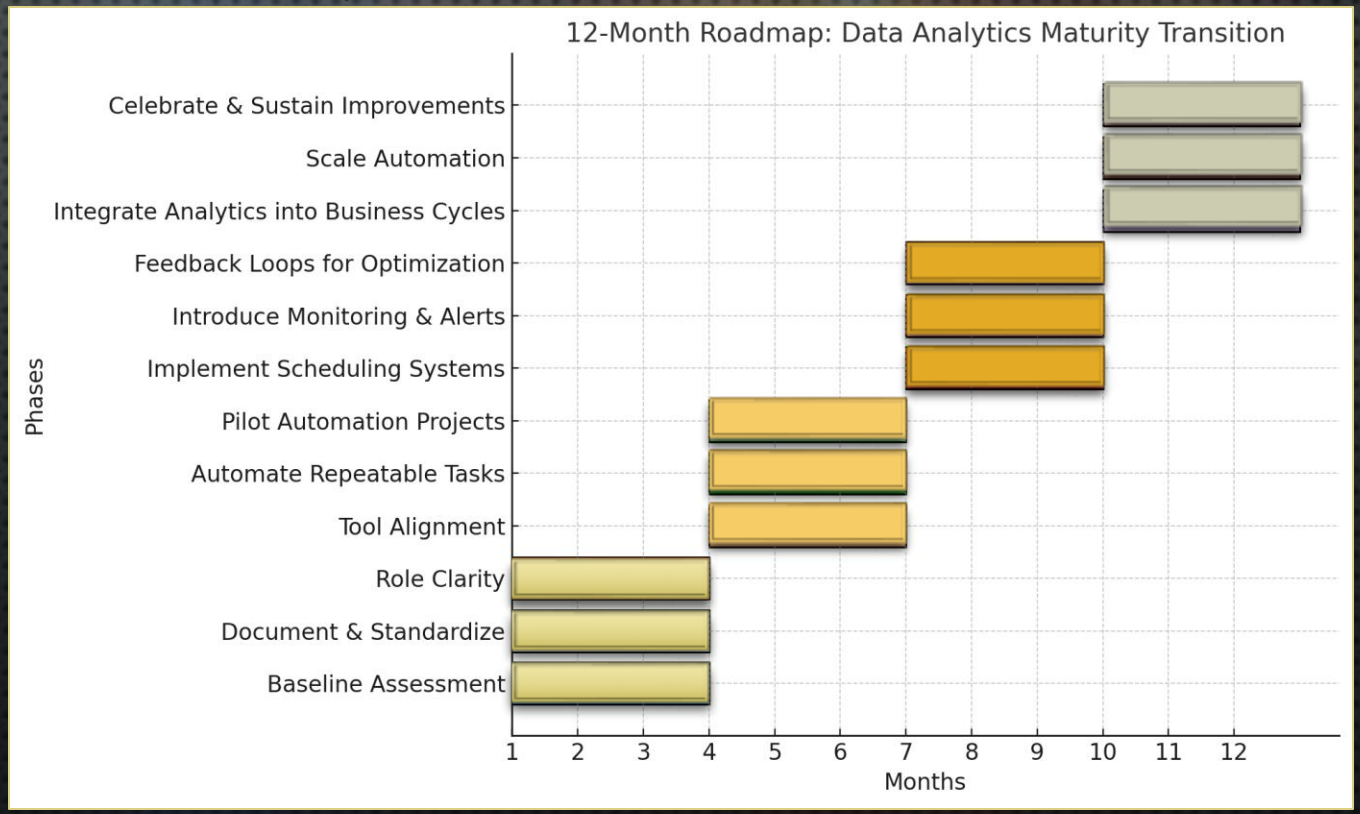
- Don’t try to ‘boil the ocean’
- Start small – focus on work that really matters and will make the biggest impact
- Identify toolsets that match team skill sets and capabilities
- Be creative and agile
- Have a plan with quick wins

Actionable Steps – Jumpstart or Elevate



Example - Actionable Steps – Elevate Maturity Roadmap





Actionable Steps – Think Like a Fraudster

Cross functional brainstorming

- How could an internal or external fraudster try to defraud the company?
- Rank schemes - easy to hard
- For top 10 easiest:
  - What would the act and/or concealment look like in the data?
  - Which one would be easiest for us to find in the data?

Actionable Steps - ChatGPT – What you need to know

- ⚠ DO NOT share sensitive, proprietary or PII information
- ⚠ Only the ChatGPT Enterprise version won't retain any input data and is SOC 2 compliant
- ⚠ Do not rely on AI for expert advice – consult the experts

- ⚠ Data used by AI is not always up to date – check real time sources
- ⚠ Outputs may be biased
- ⚠ Always verify important information before sharing it with others or using it for critical decision making

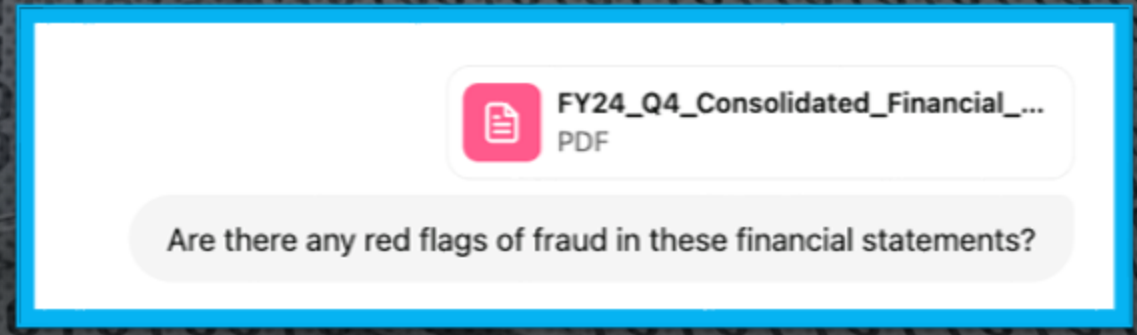
Example - Actionable Steps - ChatGPT

Prompt Examples

I am looking for red flags of fraud in journal entry transactions for a small to mid sized company. The only tool I have available is Excel. What are the 3 best ways I can use Excel to identify red flags?

I am looking for red flags of fraud in journal entry transactions for a small to mid sized company. The only tool I have available is Excel. What are the 3 best ways I can use Excel to identify red flags?

Are there any red flags of fraud in this data set?



Can you give me the fog index on these two statements?

A Call to Action

Choose one idea that inspired you:

- Embrace the art of the possible
- Don't overcomplicate the work – keep it simple
- Think like a fraudster
- Don't be afraid to experiment
- Iterate, iterate, iterate…

HIDDEN IN PLAIN SIGHT:

FIGHTING FRAUD WITH DATA ANALYTICS

Let's connect!

BETHMARA KESSLER, CFE

EXAMPLE: Generative AI Usage Policy

1. Purpose & Scope

The purpose of this policy is to establish guidelines for the responsible and ethical use of generative AI tools (e.g., ChatGPT, Microsoft Co-Pilot) in the workplace. This policy applies to all employees, contractors, and third parties using AI technologies in connection with company business.

2. Acceptable Use

Employees may use AI tools for:

- Research, content drafting, summarization, brainstorming, and workflow optimization.
- Automating repetitive tasks to enhance productivity.
- Supporting, but not replacing, human judgment in decision-making.

All AI-generated content must be reviewed for accuracy, reliability, and appropriateness before use.

3. Prohibited Use

Employees may **not** use AI tools for:

- Entering, processing, or storing **confidential, proprietary, or personally identifiable information (PII)**.
- Making **business-critical decisions** without human oversight.
- Generating **legal, financial, or medical advice** without proper review by qualified professionals.
- Automating **hiring, firing, or performance evaluations** without human intervention.
- Engaging in deceptive, misleading, or unethical practices.

4. Data Security & Confidentiality

- Employees must **never** input confidential business data, trade secrets, or personal information into AI platforms.
- AI-generated content must be considered public and non-secure unless otherwise confirmed.
- Compliance with **data protection laws and internal security policies** is mandatory.

5. Quality Control & Verification

- Employees must **fact-check AI-generated content** before using or distributing it.
- AI-generated output should not be assumed to be **accurate, unbiased, or complete**.
- All official business communications must be reviewed and approved by a qualified individual.

6. Ethical Considerations

- AI must be used in alignment with the company's **values, ethical guidelines, and compliance policies**.
- Employees must **disclose AI assistance** where applicable (e.g., AI-generated content in customer-facing materials).

EXAMPLE: Generative AI Usage Policy

7. Training & Oversight

- Employees will receive **training** on responsible AI use and associated risks.
- An AI Governance Team or Compliance Officer will oversee AI-related concerns and policy enforcement.

8. Monitoring & Enforcement

- The company reserves the right to **audit AI usage** for compliance.
- **Violations** of this policy may result in disciplinary action, up to and including termination.

This policy is subject to periodic review and updates as AI technologies evolve.

This example policy was generated by ChatGPT