



# KPMG Risk Insights Executive talk

Key thematic areas to consider  
in 2025

KPMG in Thailand

No.1/2025 – 24 January 2025



# KPMG presenters today



**Supachate  
Kunaluckkul**

CIA, CISA, CCSA, CPA

---

Consulting Partner  
Head of Enterprise Risk  
KPMG in Thailand



**Naipaporn  
Sagulyat**

CIA, CRMA, CPA, CCSA,  
CIPM, GRCA, GRCP

---

Consulting Partner,  
GRCs  
KPMG in Thailand



**Nutthapon  
Limwandee**

CFE

---

Consulting Associate Director,  
Forensic Consulting, Technology  
KPMG in Thailand



**Chanikarn  
Srithundorn**

CFE

---

Consulting Associate Director,  
Forensic Consulting, Accounting  
KPMG in Thailand



**Peerawat  
Apiratitham**

CIA, CPA, GRCA, GRCP, IAAP

---

Consulting Associate Director,  
GRCs  
KPMG in Thailand

# Agenda



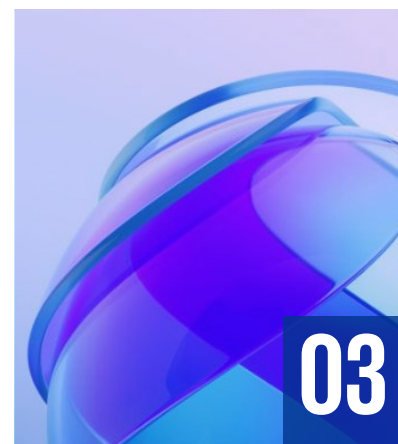
## Key thematic areas for forward-looking planning

Key areas the organization should address in the coming years



## Sharpening your detection skills in the digital age

Harness the power of digital tools for data insights and anomaly detection



## New Global Internal Audit Standards

Get ready for the implementation of new Global Internal Audit Standards



## Key takeaways and Q&A session

An exclusive conversation with KPMG Business Advisors

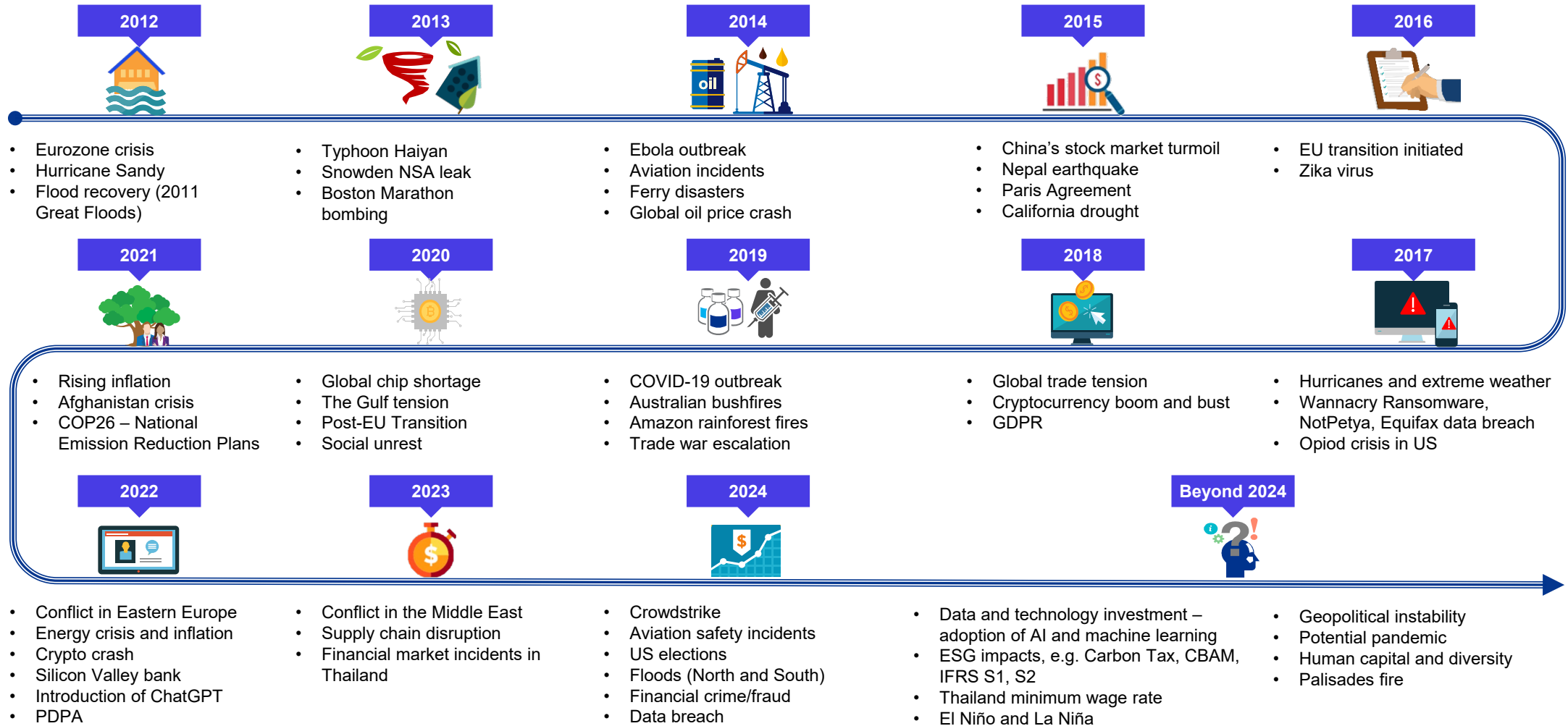
**01**

**Key thematic areas  
for forward-looking  
planning**



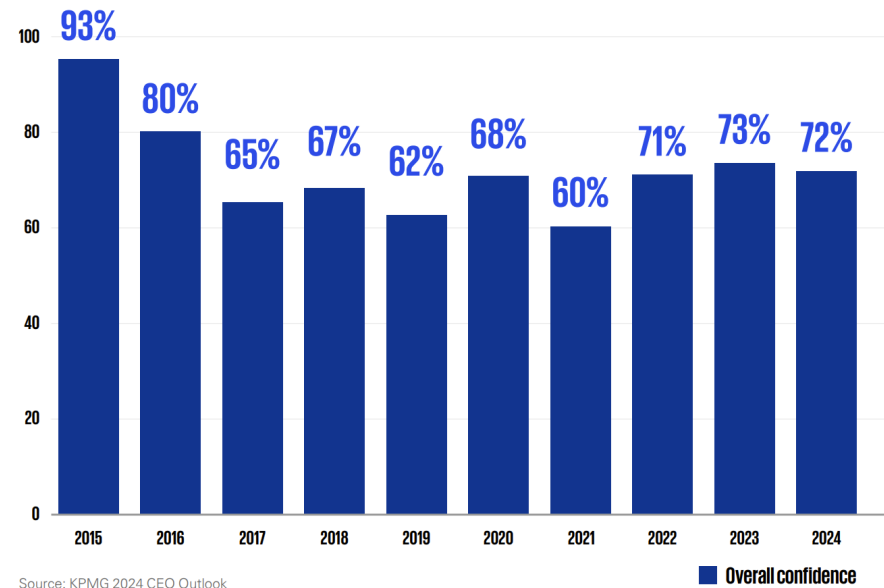
**How can we leverage our past to  
better predict and prepare for the  
future?**

# Evolving risk environment in the age of “polycrisis”

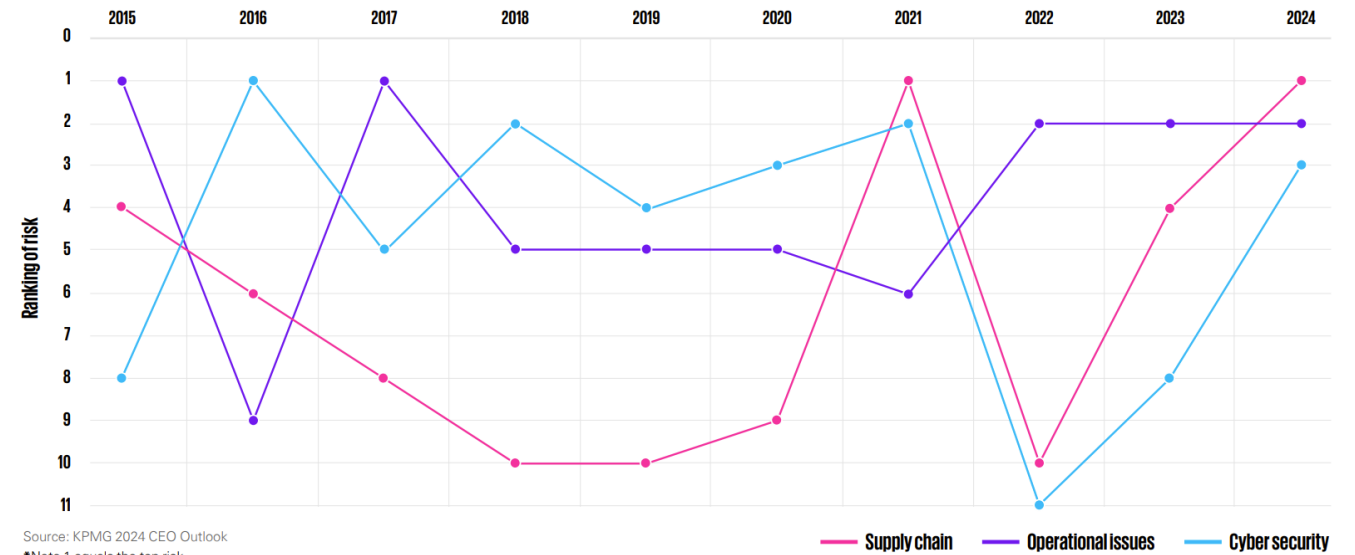


# KPMG CEO Outlook

CEO confidence in the global economy (2015-2024)



How 2024's top threats to growth have evolved over the last ten years



**64%**

of global CEOs indicated that they would invest in AI regardless of economic conditions in 2024

**76%**

of CEOs anticipate AI will not fundamentally reduce the number of jobs within their organizations over the next three years

**69%**

Have adapted the climate-related language and terminology used to meet changing stakeholder needs.

**66%**

Of CEOs admit they aren't prepared to withstand potential shareholder scrutiny.

# Key thematic areas for 2025

Organizations are facing an increasingly complex, uncertain, unpredictable, and volatile risk landscape. Below are the selected thematic areas which organizations should consider for the risks and controls in the forthcoming year.





# Key thematic areas for 2025 – external pressures



## Third-party relationships and supply chains

### Risk insights:

- Geopolitical uncertainty
- Extreme weather
- Inflation
- Evolving regulatory landscape
- Increasing stakeholder expectations

### Example of risk and control actions:

- Assess supply chain processes
- Provide advice on the sustainability of the supply chain operating model
- Determine if sufficient consideration has been given to the risks associated with current macroeconomic and geopolitical conditions
- Sole source/single source management



## Environmental, social and governance

### Risk insights:

- Increased mandating ESG disclosure, e.g. IFRS S1, S2
- Carbon neutrality and net-zero emission commitments
- Increasing stakeholders' expectations, e.g. social media, green product/services
- ESG as part of the investment criteria, e.g. PRI & ESG Investment, FTSE Russell

### Example of risk and control actions:

- Provide advice on new reporting requirements
- Assess readiness for new reporting requirements
- Provide guidance on governance, controls and processes related to ESG metrics reporting
- Align risk management capabilities with ESG risks and organizational objectives



## Economic uncertainty and geopolitical volatility

### Risk insights:

- Economics implications of geopolitical issues and wars, such as impacts on growth, inflation, financial market, logistics and supply chain, and shipping routes
- US political landscape
- Middle East dynamics

### Example of risk and control actions:

- Integrate geopolitical risk assessment as a core element in audit plans and risk evaluations
- Assess how the first and second lines address and manage risk and operational impacts associated with geopolitical volatility

# Key thematic areas for 2025 – operational challenges



## Profitability, inflation and liquidity

### Risk insights:

- Financial risks, e.g. inflation or interest rates, have been marked by intense macro economic volatility.
- The augmentation of risks related to corporate assets and cashflow presents an onerous challenge to long-term financial performance, e.g. inflated expense, liquidity management, etc.

### Example of risk and control actions:

- Review or revisit investment and financial decisions
- Review supply chain and procurement practices
- Identify, evaluate and mitigate risks associated with inflation and interest rates
- Perform scenario analysis to prepare for various adverse scenarios



## Operational resilience

### Risk insights:

- Persistent flux in economic, geopolitical and environmental conditions present new threats and opportunities to the organization.
- The resilient system may not agile enough to adapt to disruptions, preserve critical business process and ensure performance of key technologies and information systems.
- Evolving regulatory landscape

### Example of risk and control actions:

- Identify suitable response plans to address significant threats to the organization
- Thoroughly analyze and comprehend the impacts of disruptions
- Determine intolerable levels of risk and perform cost-benefit analyses for mitigation and resilience measures



## Talent management and retention

### Risk insights:

- Evolution of AI to influence job roles, operational methods, required skills, or culture
- Talent and team diversity
- Gen Z to outnumber boomers in the workplace

### Example of risk and control actions:

- Evaluate the strategies for workforce, including future skills requirements
- Comprehend the implication of employee turnover and hiring freezes
- Assess management's oversight and plans to improve employee-centric aspects

# Key thematic areas for 2025 – technology



## Cybersecurity

### Risk insights:

- The increasing sophistication of cyber threats
- Growing digitalization of customer channels
- Adoption of new technology platforms
- Expansion of sensitive data across interconnected and integrated networks

### Example of risk and control actions:

- Assess controls to mitigate cybersecurity risks and ensure that the first and second lines are continuously monitoring cybersecurity controls
- Perform control assessments against relevant regulations and standards
- Review user access management, data management, incident responses, etc.



## Data privacy and governance

### Risk insights:

- Increased awareness among customers, employees and regulators regarding data privacy rights and the measures organizations take to protect personal information
- High-profile data breaches highlight the importance of understanding key data repositories, controls and data usage
- Data breaches can lead to loss of customer trust, reputational damage and financial penalties

### Example of risk and control actions:

- Assess the data privacy protection controls within the organization
- Clarify which data is **collected** and why, where it will be **stored** and **transferred**, whether it is **secured**, how long it will be **retained**, and how it will be **disposed of**
- Review the data breach response plan and readiness, including third-party data breach response plans



## Digital disruption and emerging technology

### Risk insights:

- AI technology as part of business
- Risks associated with the ethical deployment of AI
- Continued digital transformation across industries, with cloud technology often central to these transformations

### Example of risk and control actions:

- Assess the digital transformation strategy
- Review how AI is being used and develop AI risk mitigation plans
- Establish and control AI technologies responsibly and ethically

**02**

# **Sharpening Your Detection Skills in the Digital Age**

# FRAUD landscape

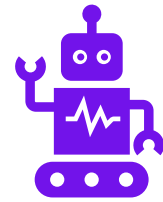
## What does the survey say?



An estimated

# 5%

of revenue is lost to FRAUD each year



The use of artificial intelligence (AI) and machine learning in anti-fraud programs is expected to nearly

## TRIPLE

 over the next two years.

# 83%

 of organizations expect to implement

## Generative AI

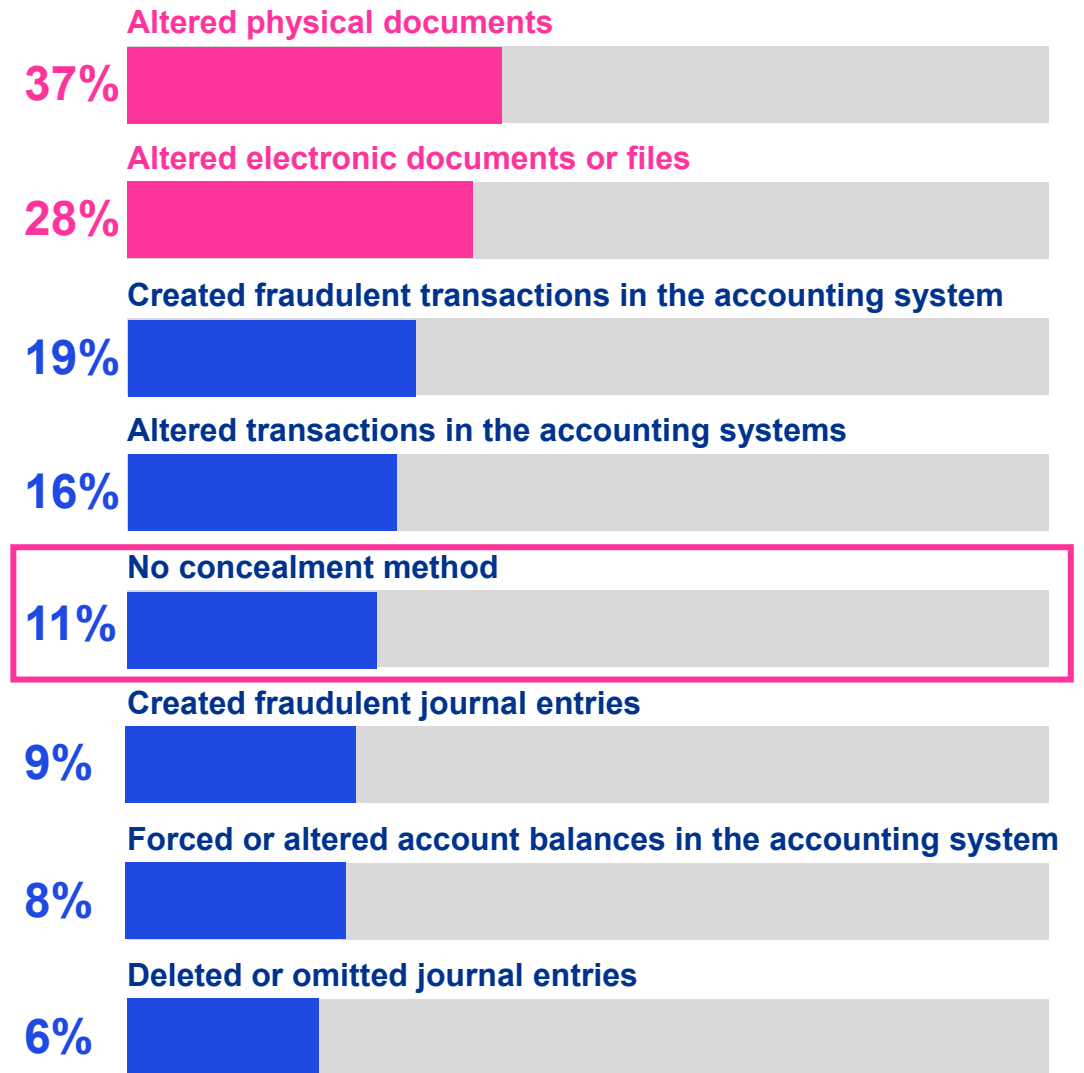
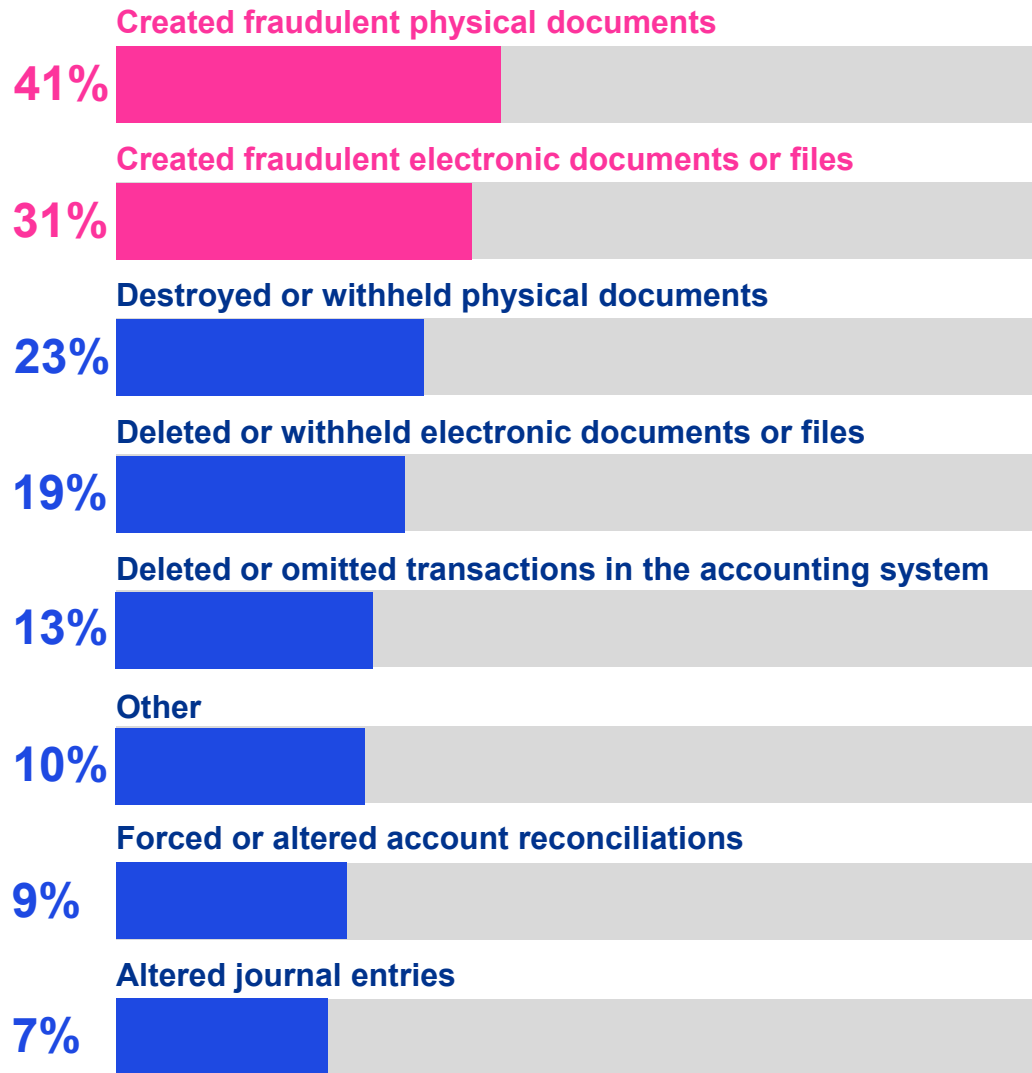
 over the next two years

### Median losses for all three primary categories of OCCUPATIONAL FRAUD increased from 2022 – 2024

	2022	2024	CHANGE
Financial statement fraud	\$593,000	\$766,000	↑ 29%
Corruption	\$150,000	\$200,000	↑ 33%
Asset misappropriation	\$100,000	\$120,000	↑ 20%

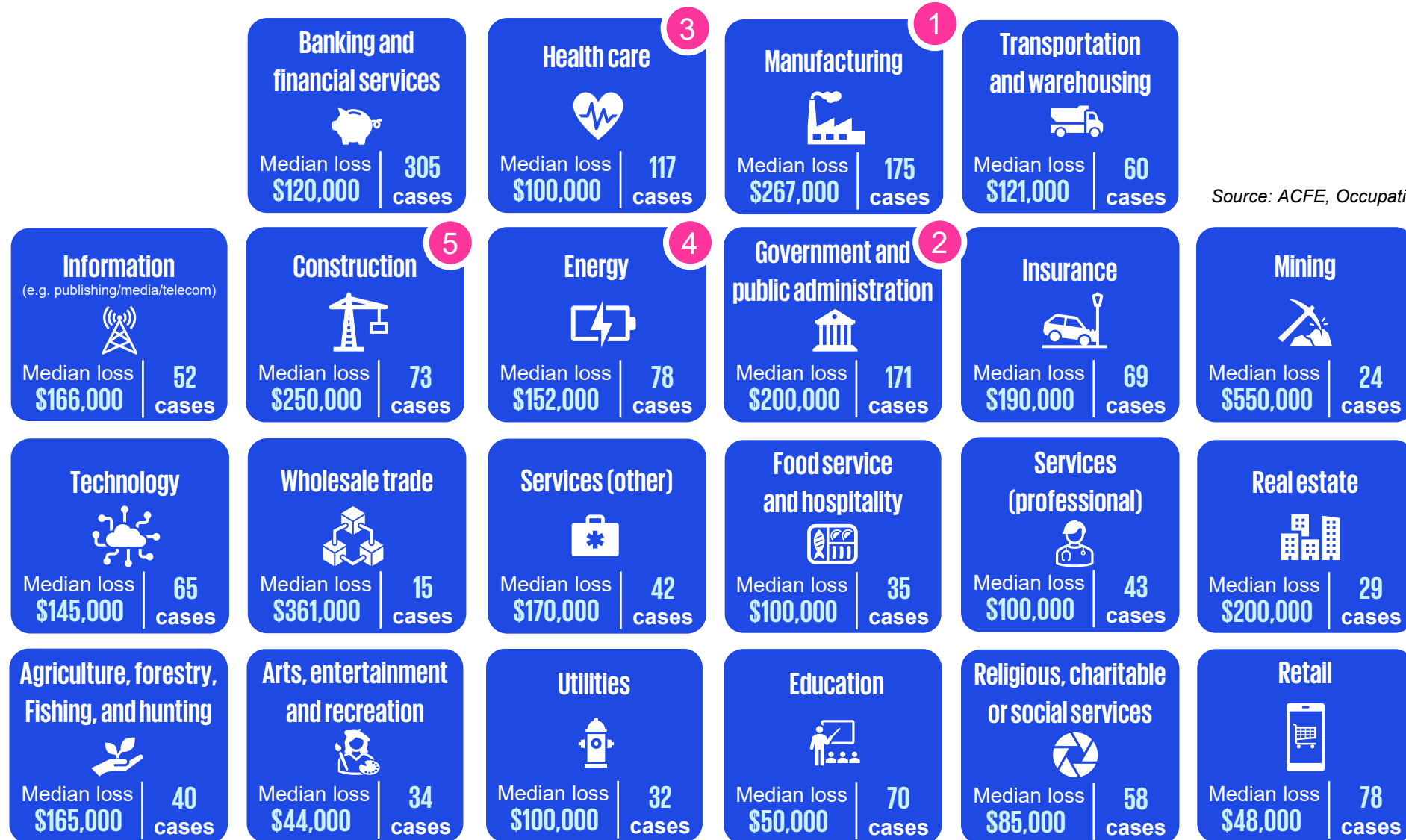
Source: ACFE, Occupational Fraud 2024

# Concealment of occupational fraud



Source: ACFE, Occupational Fraud 2024

# Occupational fraud affects organizations in different industries



Source: ACFE, Occupational Fraud 2024

# How long do different occupational fraud schemes last?

Billing

Check and payment  
tampering

Skimming

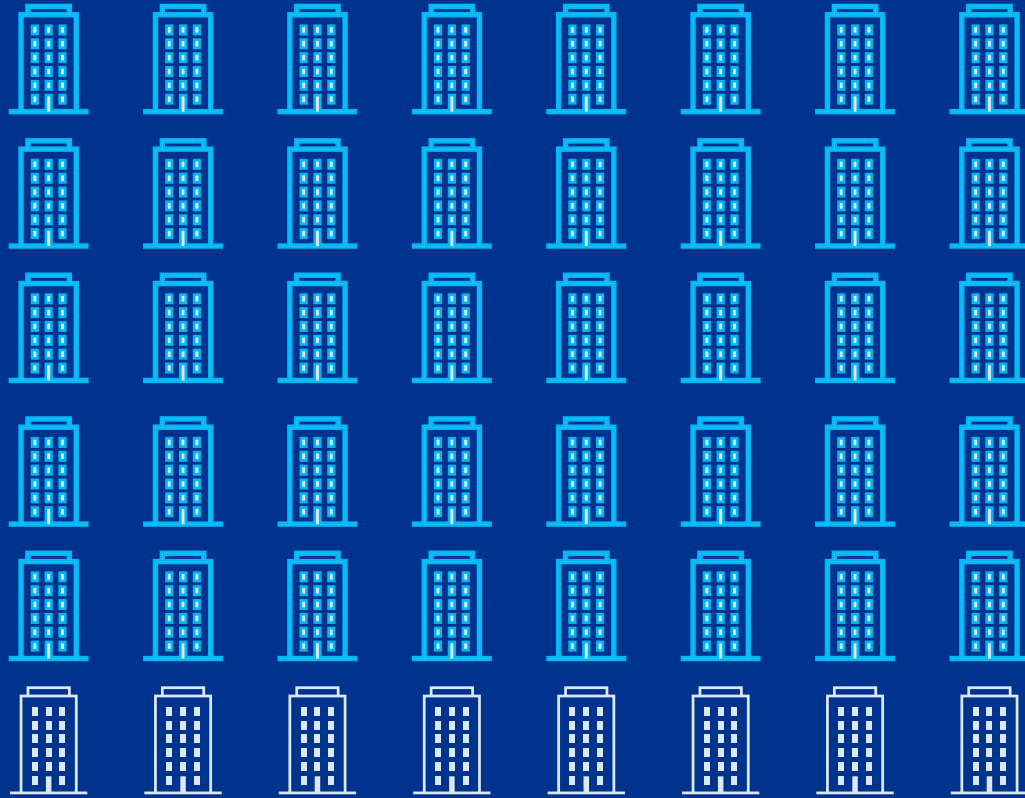
Financial statement fraud

18 months

Payroll

Expense reimbursements





**82%** of organizations  
**MODIFIED** their anti-fraud  
controls after experiencing FRAUD

# What is the most common frequency of analytics within enterprise governance at your organization?

# The most common frequency of analytics

**33%** Ad hoc/as needed

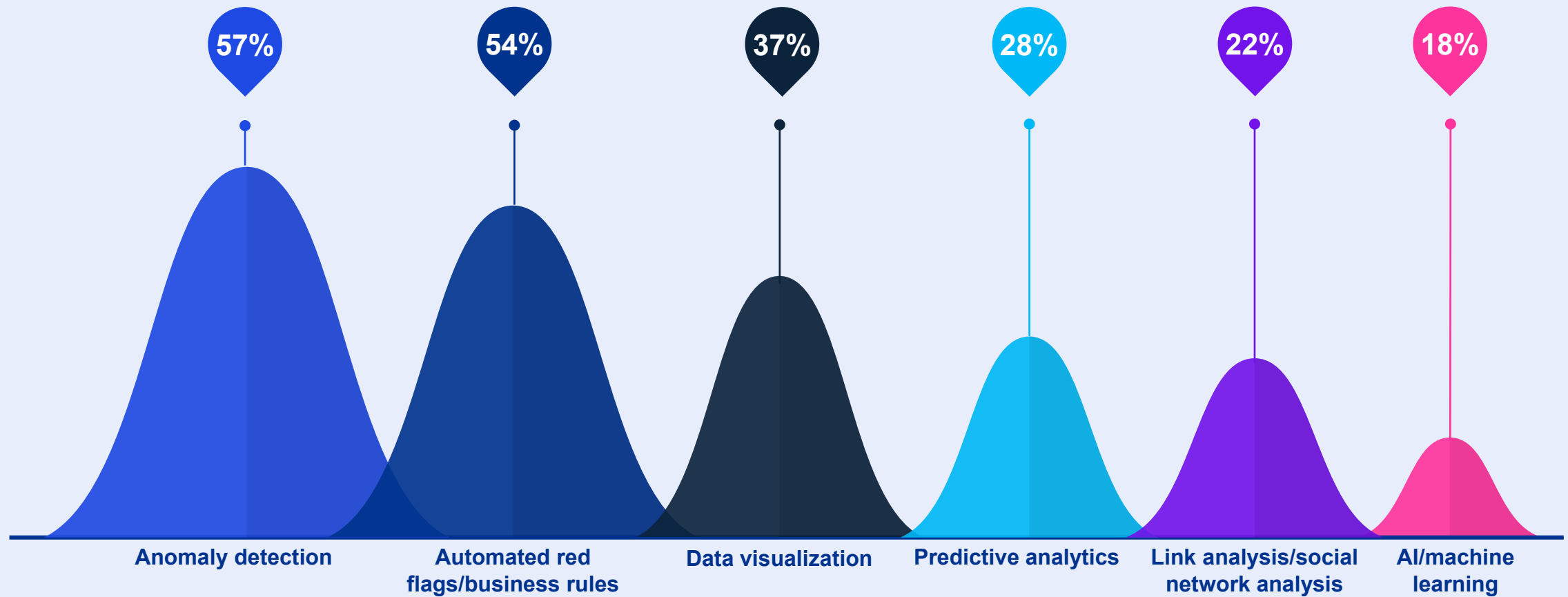
## What is the most common frequency of analytics within enterprise governance at your organization?

**20%** Monthly

**11%** Real-time

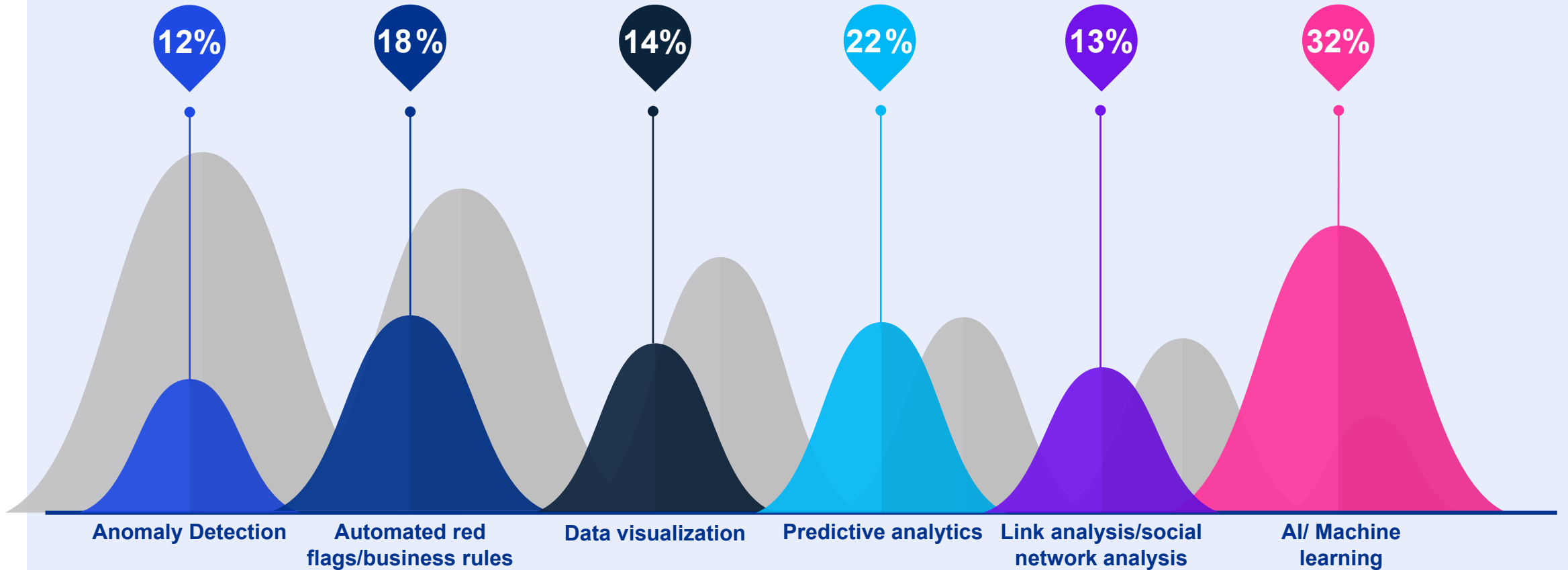
**7%** Don't currently use DA

# Top six data analysis techniques organizations currently use



Source: ACFE, 2024 Anti-Fraud Technology Benchmarking Report

# Top six data analysis techniques organizations expect to adopt in 1-2 years



Source: ACFE, 2024 Anti-Fraud Technology Benchmarking Report

# The evolution of data analytics for fraud monitoring

## Basic controls

- Policies, procedures and controls
- System reports
- Ad hoc analysis
- Sample testing
- Hotline reporting

BAU Reports

Ad hoc Reports

## Anomaly detections

- Transaction comparisons
- Aggregate risk scoring
- Text analytics
- Third party data
- Collective intelligence
- Visualization/dashboards

Transaction Comparison

Risk Scoring

IOIO  
IOIO

## Predictive models

- Real-time models
- Multivariate analytics
- Use of past fraud cases to predict future
- Hybrid-rules/predictive

Real-time Detection

Use of Past Fraud Cases

## Machine learning

- Machine learning
- Low-volume of false positives
- Automatic alerts/transaction blocking

Supervised ML

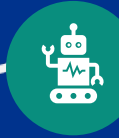
Unsupervised ML

## Business rules

- Duplicate transactions
- Threshold amounts
- 100% transactions
- Internal and third-party audits
- High volume of false positives

Threshold Amount

100% Transactions



# Result from the previous question

## Where are you at the moment?

Anomaly detections e.g. transaction comparisons, risk scoring, third party data, etc.



Basic controls e.g. ad hoc reports, hotline reports, sample testing, etc.



Business rules e.g. duplicate transactions, threshold amounts, 100% testing, etc.



Predictive models e.g. real-time detection, use of previous fraud cases, hybrid-rules, etc.



Machine learnings e.g. supervised and unsupervised techniques, etc.

# Challenges and solutions



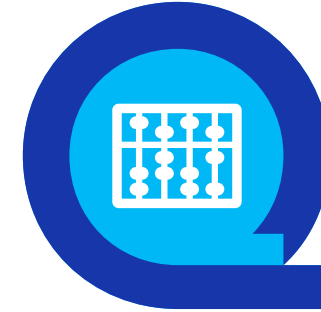
## Data availability and quality

- **Poor data quality/data consistency across system**
  - **Manual operational process**
  - **Data privacy/security issues**
- 
- Establish a clear and aligned data strategy
  - Modify process to include technology-enabled strategies
  - Communicate with IT for upcoming changes or configurations



## Capabilities and resources

- **Lack of adequate people with required skills to implement digital innovation**
- 
- Dedicated DA professional and/or up-skilling the IA team
  - Decide on a cost-effective and efficient resourcing model based on organizational structure, size and strategies



## Cost constraints

- **High costs associated with on a the digital innovation journey**
- 
- Deploy simpler innovation solutions at the onset and move to more complex procedures as the functions mature digitally

Source: KPMG



# Traditional vs data analytics and automation approach

# Quiz

2593127801398675  
7310183012819126  
1978420486742492  
7867038172175973  
7419809947623179

8<sub>s</sub>

# Quiz

2593127801398675  
7310183012819126  
1978420486742492  
7867038172175973  
7419809947623179

# Quiz

## Traditional

2593127801398675  
7310183012819126  
1978420486742492  
7867038172175973  
7419809947623179

7.55s

## Data analytics

2593127801398675  
7310183012819126  
1978420486742492  
7867038172175973  
7419809947623179

2.42s

# Traditional approaches

Rely heavily on manual methods of collecting and analyzing data

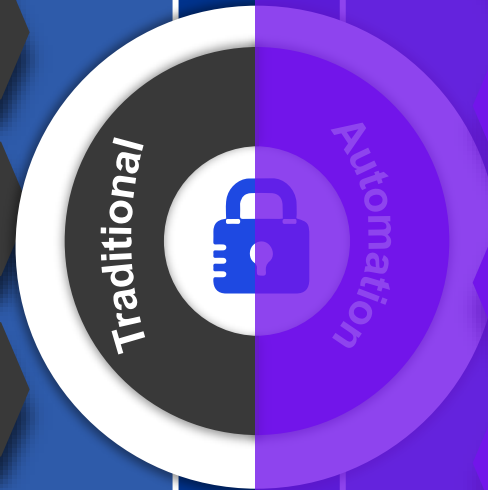
Usually on sampling basis

Dependent on reviewer's availability

Manual review of supporting documents

Dependent on skill and experience levels of the reviewer

Manual schedule of audit review period



# Automation approaches



Use technology to automate the collection and analysis of data



Conducts analysis on 100% of the data set



Review can be automated through visual monitoring platform



Focused on using data to identify trends and anomalies



Leverage machine learning to detect known fraudulent patterns and predict future suspicious activities

# Traditional approaches

Rely heavily on manual methods of collecting and analyzing data

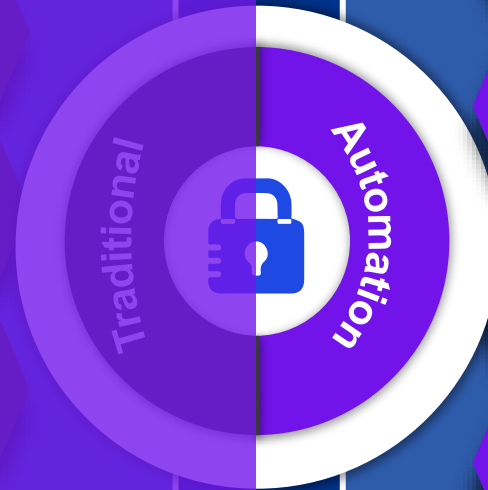
Usually on sampling basis

Dependent on reviewer's availability

Manual review of supporting documents

Dependent on skill and experience levels of the reviewer

Manual schedule of audit review period



# Automation approaches



Use technology to automate the collection and analysis of data



Conducts analysis on 100% of the data set



Review can be automated through visual monitoring platform



Focused on using data to identify trends and anomalies

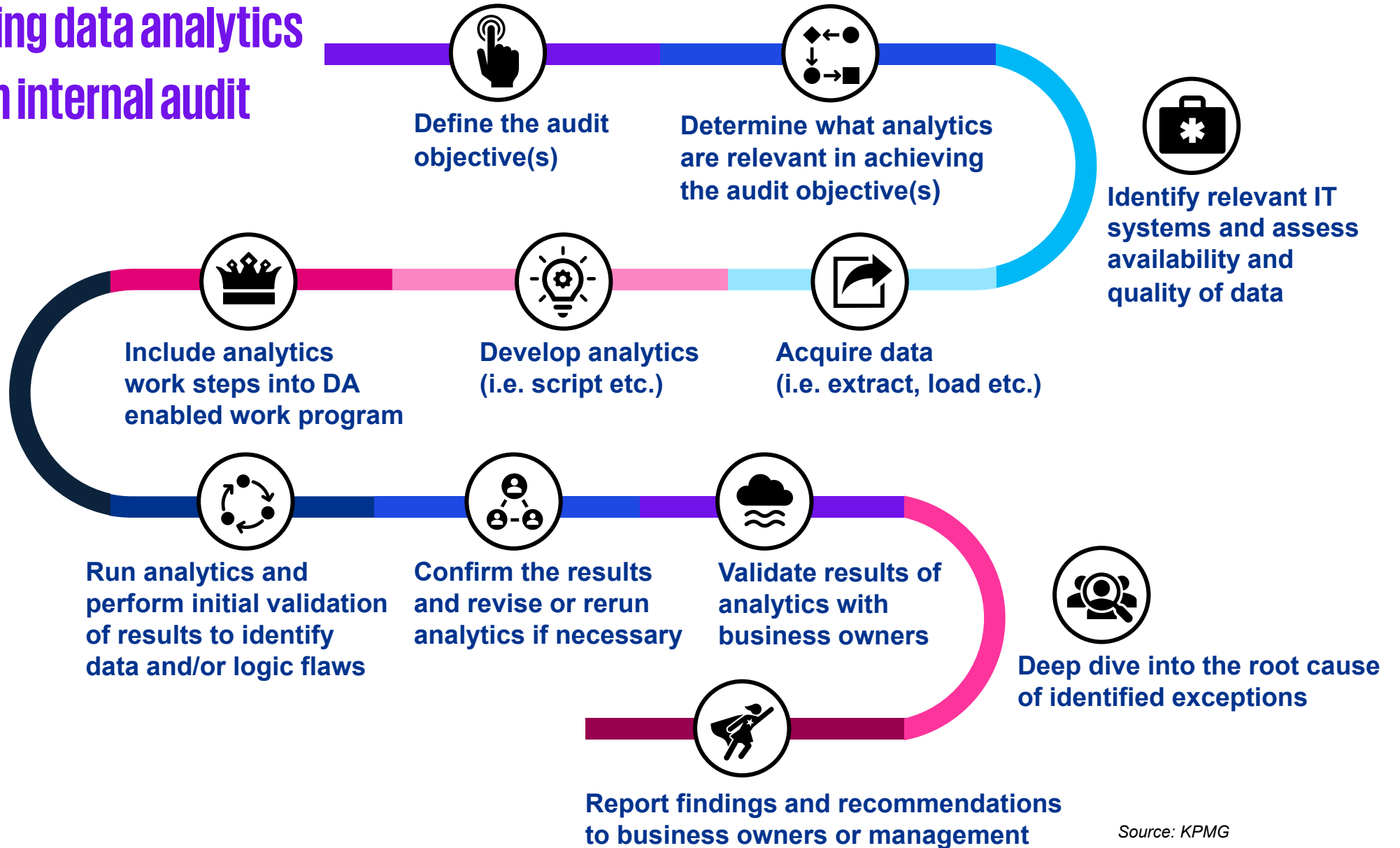


Leverage machine learning to detect known fraudulent patterns and predict future suspicious activities

# Leveraging data analytics within an internal audit

## 4 elements of successful data analytics implementation

- Data
- Tools
- People
- Processes



Source: KPMG

# Continuous auditing vs Continuous monitoring



## Continuous auditing

The combination of technology-enabled ongoing risk and control assessments. Continuous auditing is designed to enable internal auditors to **report on subject matter within a much shorter timeframe** than under the traditional retrospective approach.



## Continuous monitoring

A management process that monitors on an ongoing basis whether internal controls are operating effectively





# Our experiences in fraud monitoring



# Use case #1

## Conflict of interest

### Technique

- Exact matching
- Fuzzy matching

### Technology

- **Basic:** Power Query features
- **Advanced:** fraud monitoring tool with automated detection and visualization



Business rules

# Fraud detection powered by Power Query

## Usual scenario of the conflict of interest (shared information)

Company Alpha frequently engages with a software vendor, TechLogics, which has been *recommended by Company Alpha IT Manager, Khun Amnart*. Recently, some invoices with suspiciously high amounts from TechLogics were submitted and were *consistently and quickly approved* by Khun Amnart.

> 25%

of our clients encounter  
conflict of interest

The largest loss  
we have seen is

10 million

# Example of PowerBI Dashboard

Scenario description

Matching criteria



## Conflict of Interest Review

**Scenario Description:** When personal information is shared between suppliers and employees, it can lead to conflicts, including favoritism which may **jeopardize fair decision-making**. This might encompass situations like accepting low-quality goods, unfair pricing, or ignoring better supplier alternatives.

### Employee sharing information with Supplier (Matching Criteria)

Name Match	Address Match	Phone Match	Bank Acc Match
1	4	8	4



Detected number of matched employee and suppliers

### Employee Master

Total No. of Matched Employee

17

Match Type	Employee ID	Employee Name	Title	Address	Country	Phone No.	Bank Account
Bank Match	150	Marlow Winne	Accountant	9184 Charing Cross Plaza, Melbourne	Australia		133943341
Bank Match	18	Clayden Marge	Marketing Manager	3952 Eagan Circle, Launceston	Australia		428373267
Bank Match	198	Godridge Laryssa	Structural Engineer	98 Lien Place, Eastern Suburbs	Australia		293877213
Name Match	362	Spilling Nevil	Senior Executive	73 Dexter Way, San Juan	CR	(382) 9786016	344353621

### Supplier Master

Total No. of Matched Supplier

17

Match Type	Supplier ID	Company Name	Contact Name	Address	Country	Contact No.	Bank Account	No. of PO Doc	PO Value
Name Match	337	Basic Supply Co., Ltd.	Spilling Nevil	764 Gerald Terrace, San Juan	CR	(817) 4115731	252294721	1	3,024,054.00
Bank Match	24	G'day, Mate	Wendy Mackenzie	170 Prince Edward Parade Hunter's Hill	Australia	(02) 555-5914	293877213	3	1,206,947.40

Matched information

Purchase orders of the matched suppliers with their total transactions and values

### No. of PO Transactions

61

### Total PO Value

11,490,755

Supplier ID	PO Document	PO Date	Material No.	Material Description	Order Qty	Order Unit	Order Net Value
24	0500908900000100	Tuesday, May 23, 2023	3FBAD1N27PK01B0	100X1437D-11307 YELLOW FELTY BROTH-00	1,200.00	CAR	1,202,837.40
337	0500526138000100	Tuesday, June 22, 2021	3DE0408280077	BRD(CPF)-VN-GPE-SNS-10I*1KG(30PC)34G A4*	900.00	CAR	3,024,054.00
34	0500587706000200	Monday, October 11, 2021	LVK-121125	Chicken Haravana (280-300)PC	19.00	KG	3,800.00



# Use case #2

## Fraud scoring

### Technique

- Weighting and risk scoring

### Technology

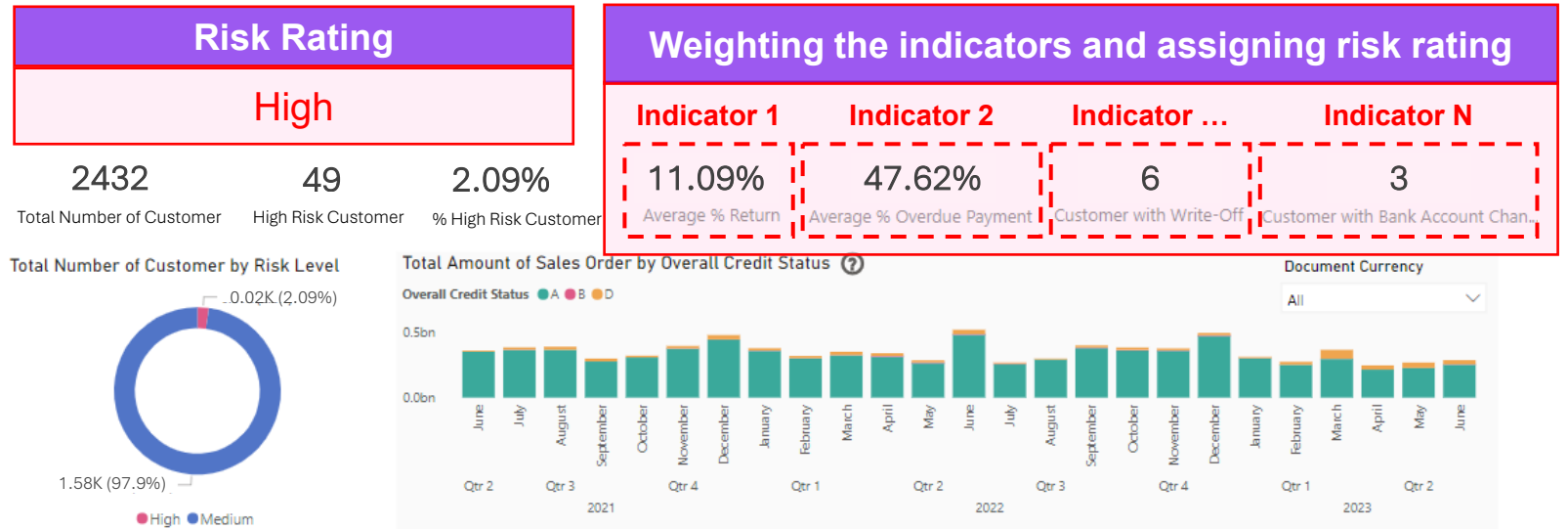
- **Basic:** Power Query features
- **Advanced:** fraud monitoring tool with automated detection and visualization



# Meaningful insights improve decision-making

## Usual scenario of fraud scoring

When reviewing red flag or alert transactions, the high volume of detected transactions can be overwhelming and mentally exhausting. It is essential to remain focused in such situations. Fraud scoring can support analysts in making informed decisions and help prioritize the highest-risk transactions.



*Embedding risk scoring into the business rules provides meaningful insights for analysts and guides them to highest-risk transactions.*

# Use case #3

## Bid rigging

### Technique

- Association rule mining

### Technology

- **Basic:** Excel with add-ins or plug-in features
- **Advanced:** fraud monitoring tool with automated detection and visualization

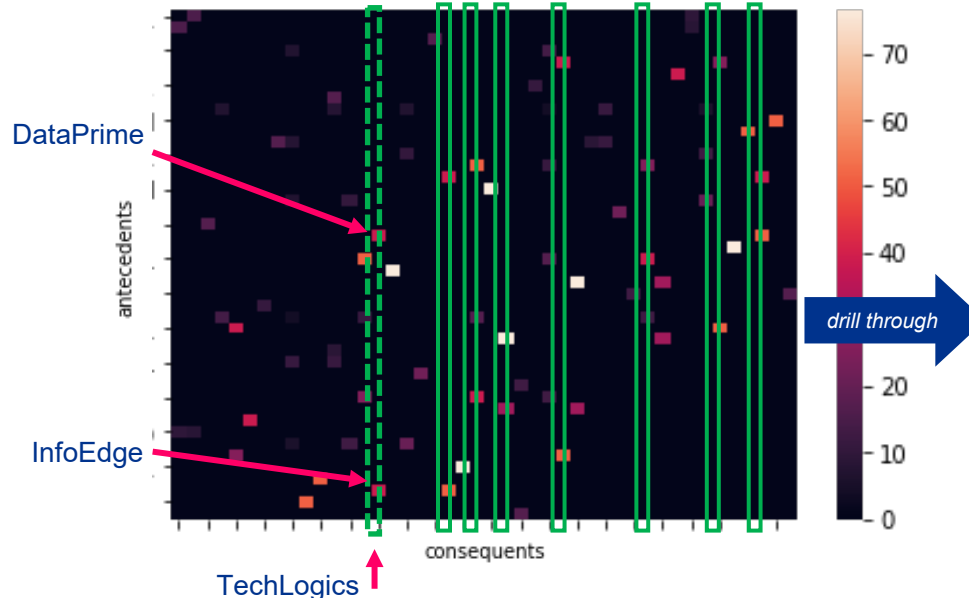


# Pattern of bid rigging using AI-technique

## Usual scenario of bid rigging

In Metropolis city's IT project, three leading tech firms, TechLogics, InfoEdge and DataPrime, are participating in a bidding. Behind the scenes, an illicit agreement is formed. *TechLogics*, the predetermined 'winner', submits a competitive bid while InfoEdge and DataPrime, acting as 'nominee' bidders, submit high, non-competitive bids.

Heatmap showing the relationship of vendors:



Bidding information				
Date	Candidate 1	Candidate 2	Candidate 3	Awarded
2-Jan-22	TechLogics	InfoEdge	DataPrime	TechLogics
...	...	...	...	...
...	...	...	...	...
...	...	...	...	...
7-Jun-22	InfoEdge	TechLogics	DataPrime	TechLogics
...	...	...	...	...
6-Feb-23	TechLogics	DataPrime	InfoEdge	TechLogics
...	...	...	...	...
...	...	...	...	...
3-Aug-23	InfoEdge	TechLogics	DataPrime	TechLogics
...	...	...	...	...
9-Nov-23	DataPrime	InfoEdge	TechLogics	TechLogics

# Use case #4

## Behavior analysis

### Technique

- Segmentation
- 1.5xIQR Rule

### Technology

- **Advanced:** fraud monitoring tool with automated detection and visualization

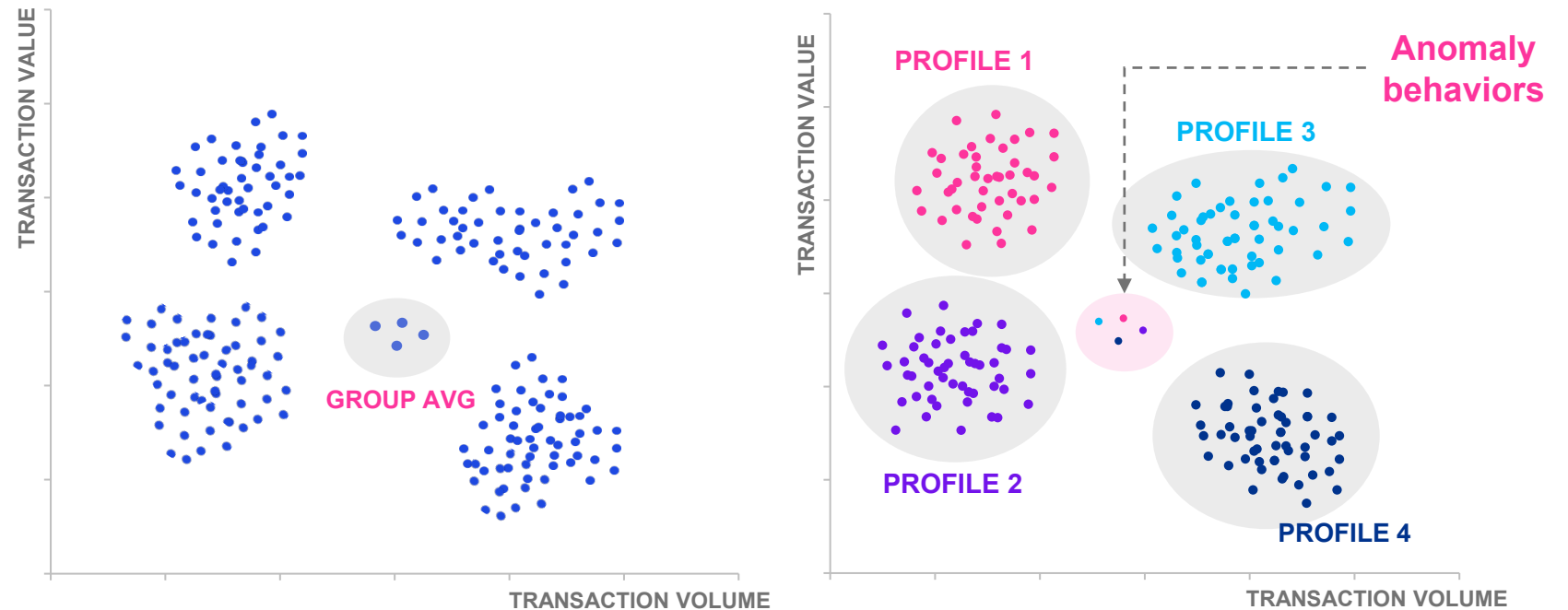
 Predictive models

 Machine learning

# Behavior analysis, I know what you did last summer

## Usual scenario of anomalies

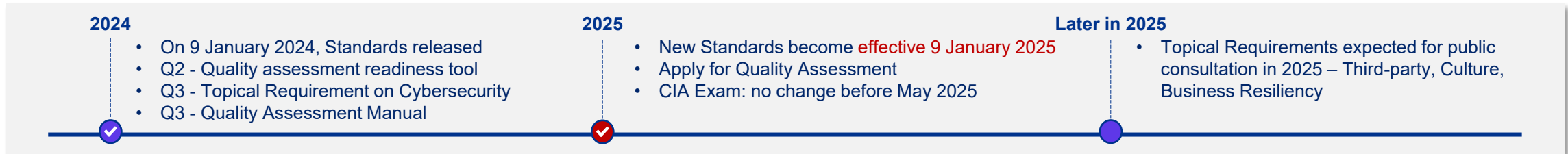
At TechLogics Ltd., the finance department *noticed an anomaly* — Sales Representative Khun Anurak consistently reported unusually high expenses, mainly for client meals and entertainments, compared to other sales representatives in the same coverage area.



**03**

# **New Global Internal Audit Standards**

# Global Internal Audit Standards – Key insights



The Standards combine into one document the five mandatory components of 2017 IPPF (Mission of Internal Audit, Definition of Internal Auditing, Core Principles for the Professional Practice of Internal Auditing, Code of Ethics, and Standards), as well as one of the recommended non-mandatory elements, the Implementation Guidance.

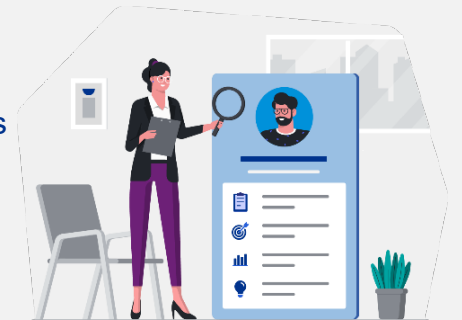
## ONE DOCUMENT

Encompasses the following elements from the 2017 IIA Standards into one framework:

- *Mission of Internal Audit*
- *Definition of Internal Auditing*
- *Core Principles for the Professional Practice of Internal Auditing*
- *Code of Ethics*
- *Standards*
- *Implementation Guidance (recommended)*

## NOTABLE CHANGES

1. Essential Conditions for Board and Senior Management
2. Internal Audit Strategy
3. Integrated Assurance and the Internal Audit Plan
4. Report and Finding Ratings
5. Performance Measurement
6. Technology Enhancement
7. Enhanced External Quality Assessments





# Global Internal Audit Standards – Key insights

1

What are the **key changes** to the IIA Standards and How does the Internal Audit Team **align with** the new standards?

2

Does the Internal Audit Team have a **clear and documented implementation plan** for the compliance with the new standards?

3

What **resources** (people, process, technology) are required to implement the new standards and does the Internal Audit Team have **sufficient and necessary skills** for compliance with the standards?

4

What **training programs or professional development** will be needed for the internal audit team?

5

Is the **key stakeholders** (Board, Audit Committee, Senior Management) aware, fully informed, and supportive for the implementation?

**04**

# **Key Takeaways and Q&A Session**

# Key thematic areas to consider in 2025



Become more predictive and agile to effectively respond to the evolving risk landscape and the age of the “Polycrisis”




Anticipate and address operational challenges in this digital age



Leverage AI, Machine Learning, and Data Analytics including GRC Transformation tools, to manage the risks and controls of the organization more effectively and efficiently, while enhancing fraud monitoring and detection capabilities of the organization.



Prepare and ready for compliance with the new Global Internal Audit Standards which become effective on 9 January 2025

The background of the left panel features a stylized globe with a grid of dots and lines, overlaid on a bar chart with vertical bars of varying heights. A white line graph with circular markers is also visible, tracing a path across the data points.

**Key thematic areas  
to consider  
in 2025**

**Questions &  
Answers**



Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**KPMG in Thailand**

48<sup>th</sup>-50<sup>th</sup> Floor, Empire Tower  
1 South Sathorn Road  
Bangkok 10120  
T: +66 2677 2000



KPMG in Thailand



[kpmg.com/th](https://kpmg.com/th)

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

©2025 KPMG Phoomchai Business Advisory Ltd., a Thai limited liability company and a member firm of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

**Document Classification: KPMG Public**