

# Full-Court Press: Defending Against Third Party AI Risk



**Co-founder & CPO**

**FABRIK**

the team behind [GenAITrust.com](https://GenAITrust.com)

Hi! I'm Henry Stanley.

Previously, led:

- FISMA High & PCI Compliance at CLEAR
- Developer Experience Products at Spotify
- Data Science Products at Aetion

**I'm on a mission to solve B2B trust.**



We asked 87 Enterprise Risk leaders about how they're approaching AI risk.



The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces of the stone.

**"AI is changing the game  
for vendor risk."**

# 77%

of SaaS Vendors

BUILT AI FEATURES IN 2023

Source: OpenView

# 500+

SaaS Vendors

AT \$100M+ ENTERPRISES

Source: We asked dozens of \$100M enterprises.

# 3/10

SaaS Vendors

DISCLOSE AI USE IN THEIR  
TERMS OF SERVICE

Source: We read hundreds of ToS.

The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces of the stone.

**Why should we care  
about vendor AI risk?**

# Recap: two types of AI in use today

## Reactive Machine AI



- No memory
- Narrow reasoning
- Specific tasks



- Recommendations
- IBM Deep Blue



**Known quantity**



# Recap: two types of AI in use today

## Reactive Machine AI



- No memory
- Narrow reasoning
- Specific tasks



- Recommendations
- IBM Deep Blue



Known quantity

## Limited Memory AI



- Some recall
- Diverse reasoning
- Broad tasks



- Generative AI
- Chatbots
- Self-Driving Cars



New & novel risk

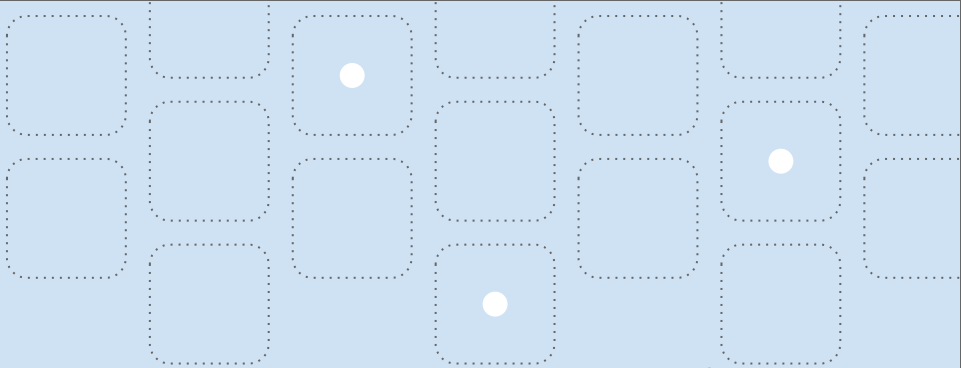


The background of the slide is a close-up photograph of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces of the stone.

Why should we care about vendor AI risk?

**Reason #1: AI risk  
is multi-faceted**

# Security risks with AI models



Data Poisoning

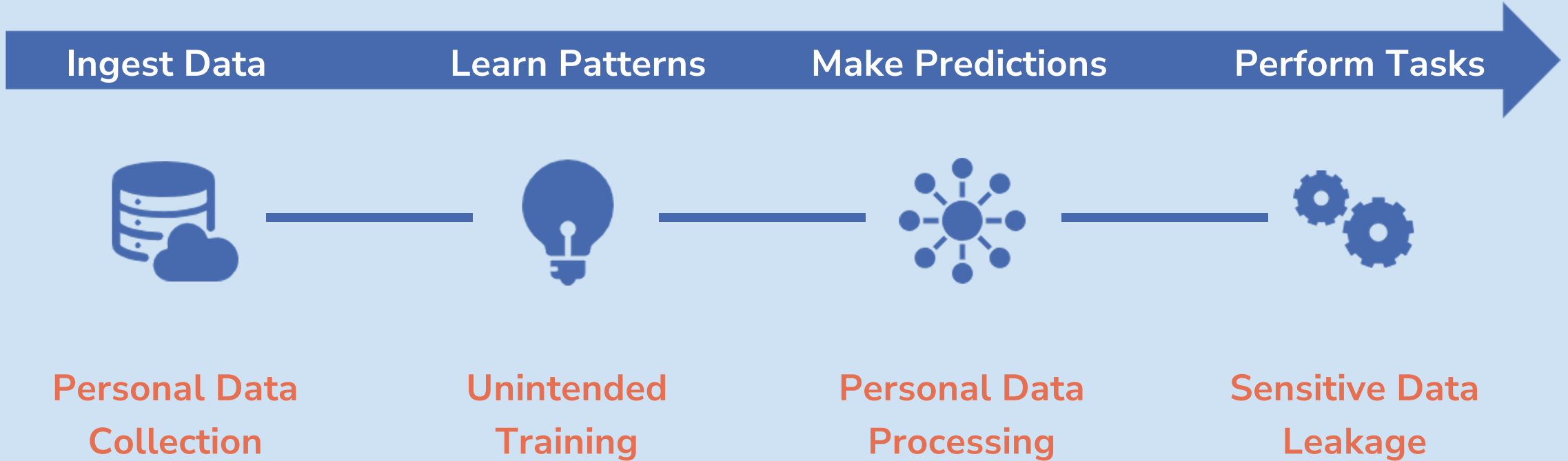
Excessive Data  
Retention

Prompt Injection

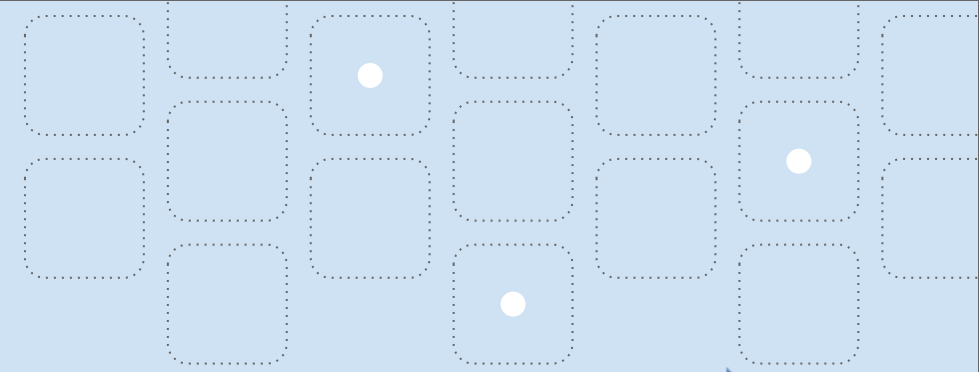
Insecure Output  
Handling



# Data privacy risks with AI models



# Legal risks with AI models



Ingest Data

Learn Patterns

Make Predictions

Perform Tasks



Improper Training  
Data

IP Infringement

Unanticipated Data  
Retention

Ownership of  
Output



# Ethical & safety risks with AI models

Ingest Data

Learn Patterns

Make Predictions

Perform Tasks



**Skewed  
Representation**

**Bias  
Amplification**

**Unexplainable  
Outcomes**

**Lack of Human  
Oversight**



The background of the image is a close-up of a grey, textured stone surface with numerous dark, irregular cracks forming a network across the entire frame. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces of the stone.

Why should we care about vendor AI risk?

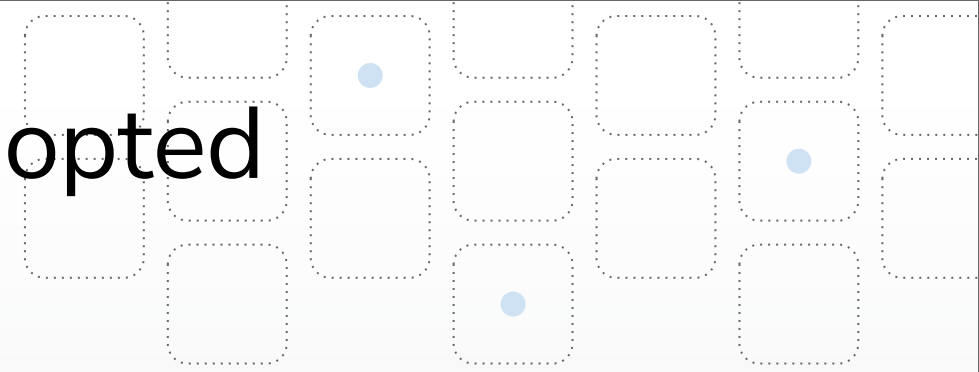
**Reason #1: AI risk is  
multi-faceted**

The background of the slide is a close-up photograph of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces.

Why should we care about vendor AI risk?

**Reason #2: AI governance  
standards aren't widely adopted**

# Standards are new and barely adopted



## New Governance Frameworks

- NIST AI RMF
- ISO 42001
- OWASP Top 10 for LLMs
- Cloud Security Alliance AI Safety
- & many more

## Expanding Regulation

- EU AI Act
- CA Bill AB-302
- NYC LL 144
- & more globally



77%

of SaaS Vendors

BUILT AI FEATURES IN 2023

Source: OpenView

3/10

SaaS Vendors

DISCLOSE AI IN THEIR TERMS OF  
SERVICE

Source: We read hundreds of Terms of Service

The background of the slide is a close-up photograph of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces.

Why should we care about vendor AI risk?

**Reason #2: AI governance  
standards aren't widely adopted**

The background of the image is a close-up of a grey, textured stone surface with numerous dark, irregular cracks. The cracks form a complex, interconnected pattern across the entire frame. The lighting is somewhat uneven, with darker areas in the shadows of the cracks and lighter areas on the raised surfaces of the stone.

Why should we care about vendor AI risk?

**Reason #3: AI adoption is  
spreading very quickly**

# Terms of Service drift creates new risks



# Terms of Service drift creates new risks



March 31, 2023

**Terms of Service disclosed use of  
Customer Content for training AI**



# Terms of Service drift creates new risks



March 31, 2023

**Terms of Service disclosed use of  
Customer Content for training AI**



August 7, 2023

**Public Backlash**



# Terms of Service drift creates new risks



March 31, 2023

**Terms of Service disclosed use of Customer Content for training AI**



August 11, 2023

**Terms amended to prohibit use of Customer Content for training AI**



August 7, 2023

**Public Backlash**



# Terms of Service drift creates new risks



March 31, 2023  
Terms of Service disclosed use of  
Customer Content for training AI

133 days of unmitigated risk



August 11, 2023  
Terms amended to  
prohibit use of Customer  
Content for training AI



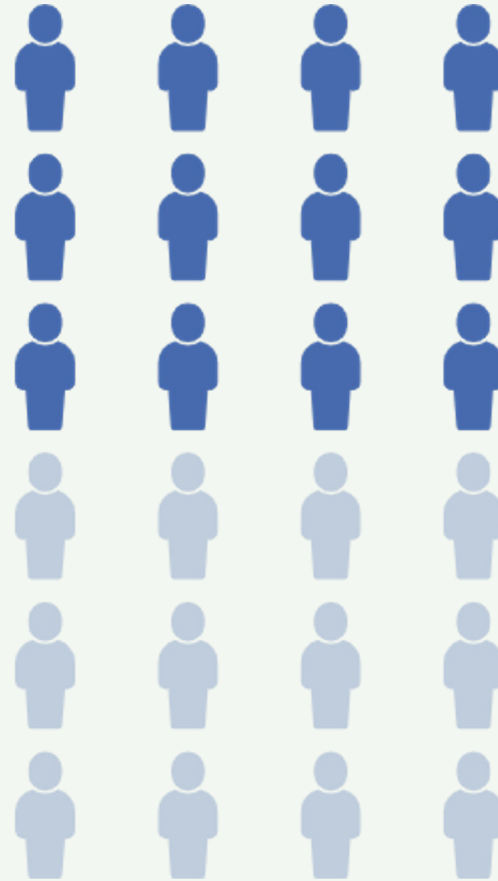
August 7, 2023  
Public Backlash





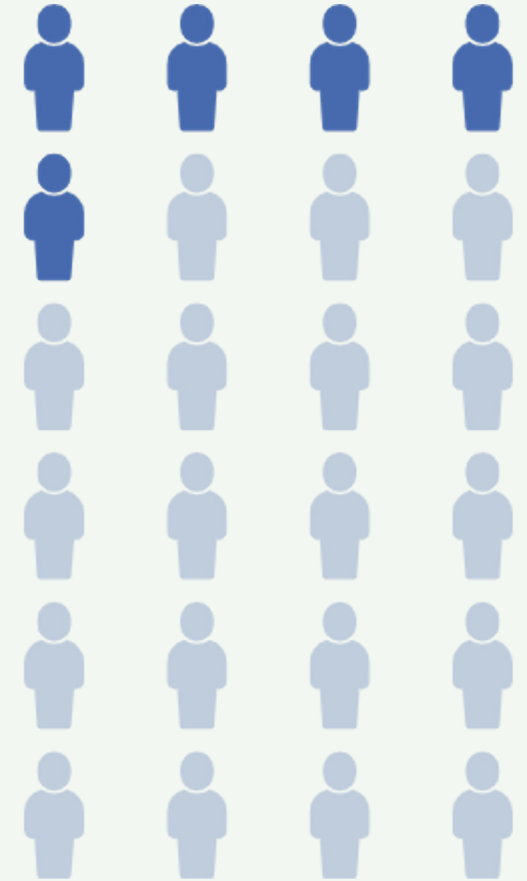
Gen AI use is **more extensive** than you think.

49%



49% of employees are using generative AI, with 33% using it **weekly**.

18%




Only 18% say company shared any AI acceptable usage policies.

The background of the slide is a close-up photograph of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces.

Why should we care about vendor AI risk?

**Reason #3: AI adoption is  
spreading very quickly**

The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces.

Dozens of Vendor Risk leaders  
told us the same things.


The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the crevices and lighter tones on the raised surfaces of the stone.

"It'll take me months to inventory vendor AI systems."

"Our risk assessments are quickly outdated."

"We're not keeping up with the business."

"We're still figuring it out."

The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the crevices and lighter tones on the raised surfaces of the stone.

The way we were taught to manage  
vendor risk is suited  
**for a world that no longer exists.**



## What usually works for vendor risk...

- Standard compliance frameworks
- Security questionnaires
- 1-2 year review cycles
- Third-party audits



## ...isn't ready for AI.

- Standard compliance frameworks
- Security questionnaires
- 1-2 year review cycles
- Third-party audits

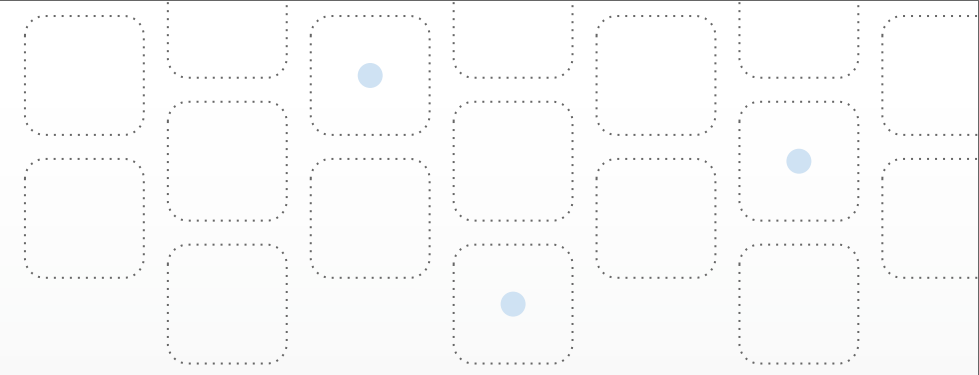
The background of the image is a close-up of a stone surface, possibly a wall or floor, characterized by a network of dark, irregular cracks that divide the surface into irregular, polygonal shapes. The stone has a mottled appearance with various shades of grey, blue-grey, and brownish-tan, suggesting a natural, weathered material.

**AI is a global risk event.**



The background of the image is a close-up of a grey, textured stone surface, possibly marble or granite, characterized by a network of dark, irregular cracks that create a mosaic-like pattern. The lighting is somewhat uneven, with darker tones in the shadows of the cracks and lighter tones on the raised surfaces of the stone.

We need a plan for  
third party AI risk.



Here's how we can  
get started.





**1**

**Align to AI risk frameworks**

**2**

**Build a third party AI inventory**

**3**

**Monitor vendors for changes**



Gen AI Trust [Network](#)  
at **GenAITrust.com**



1

Align to AI  
Risk  
Frameworks



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)



1

# Align to AI Risk Frameworks

## Leading frameworks share vendor risk guidance

**NIST**

**AI RMF 1.0**

- Govern 6.1
- Govern 6.2
- Manage 3.1
- Map 4.2



**42001:2023**

- Article 13
- Article 25



**EU AI Act**

- Annex A B.6
- Annex A B.8
- Annex B.10





1

# Align to AI Risk Frameworks

Leading frameworks share vendor risk guidance

**NIST**

**AI RMF 1.0**



**42001:202**

**3**



**EU AI  
Act**

## Shared Requirements

- Define policies & procedures for third party AI
- Provide guidance for using AI systems
- Inventory third party AI systems
- Document & manage risks



1

Align to AI risk frameworks

2

Build a third party AI inventory

3

Monitor vendors for changes



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)



2

Build a third  
party AI  
inventory



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)





2

## Build a third party AI inventory

Take inventory to understand your exposure

### Start with:

- Identify third party AI used across the org
- Understand data types involved
- Define your risk categories
- Collect vendor risk data





2

Build a third  
party AI  
inventory

The vast majority of AI risk assessments start with the same questions.



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)

# Common AI risk assessment questions

2

Build a third  
party AI  
inventory



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)



2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



Gen AI Trust [Network](#)  
at [GenAITrust.com](https://GenAITrust.com)



2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



### Notice

Are users notified when they are interacting with an AI feature?





2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



### Notice

Are users notified when they are interacting with an AI feature?



### Consent

Is user opt-in consent required to interact with AI features?





2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



### Data Reuse

Does the company train AI models on customer data?



### Notice

Are users notified when they are interacting with an AI feature?



### Consent

Is user opt-in consent required to interact with AI features?





2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



### Data Reuse

Does the company train AI models on customer data?



### Notice

Are users notified when they are interacting with an AI feature?



### Data Retention

How long is data retained for AI use, and where is it stored?



### Consent

Is user opt-in consent required to interact with AI features?







2

Build a third  
party AI  
inventory

## Common AI risk assessment questions



### Transparency

Does the vendor disclose any use of AI in their ToS or PP?



### Data Reuse

Does the company train AI models on customer data?



### Notice

Are users notified when they are interacting with an AI feature?



### Data Retention

How long is data retained for AI use, and where is it stored?



### Consent

Is user opt-in consent required to interact with AI features?



### Data Sharing

Do any third parties process customer data for AI use?





2

## Build a third party AI inventory

# Challenges building your AI inventory



Keeping up with AI development



Time & effort to collect data



Inventory freshness



Adequate coverage



Business ownership





1

Align to AI risk frameworks

2

Build a third party AI inventory

3

Monitor vendors for changes



Gen AI Trust [Network](https://www.GenAITrust.com)  
at **GenAITrust.com**



3

**Monitor  
vendors for  
changes**



Gen AI Trust [Network](#)  
at [GenAITrust.com](#)

# Monitoring is crucial to manage drift

3

Monitor  
vendors for  
changes

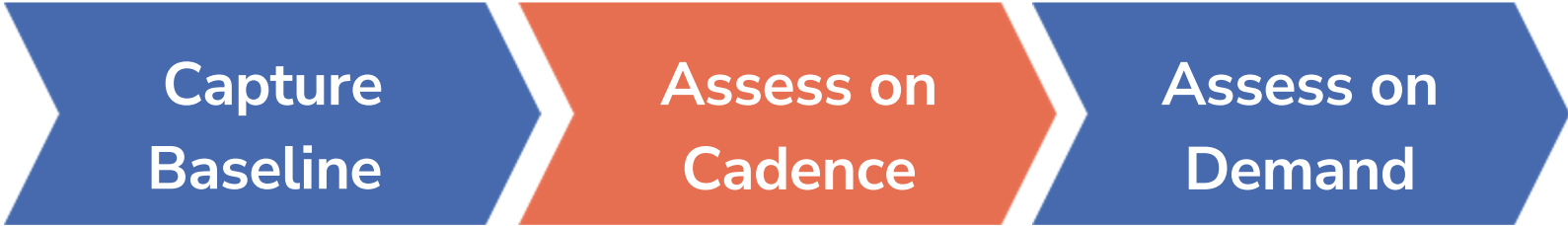
Capture  
Baseline

Assess on  
Cadence

Assess on  
Demand



The rate of vendor change is accelerating



3

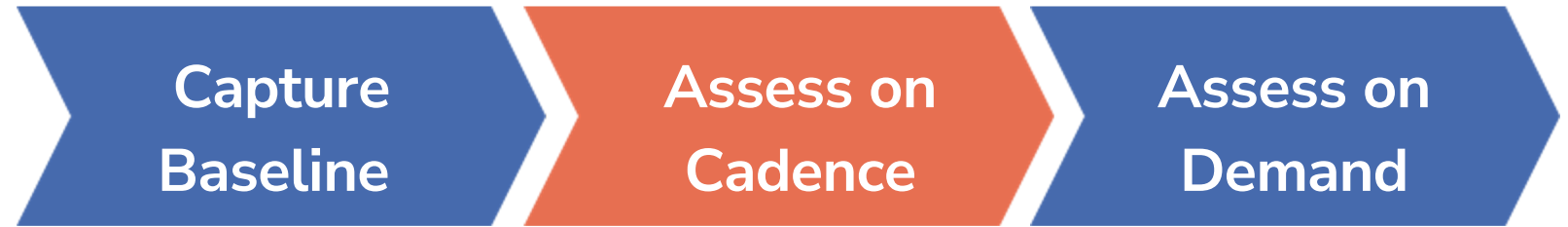
Monitor vendors for changes



3

Monitor  
vendors for  
changes

The rate of vendor change is accelerating



Predictable

Unresponsive

Stale



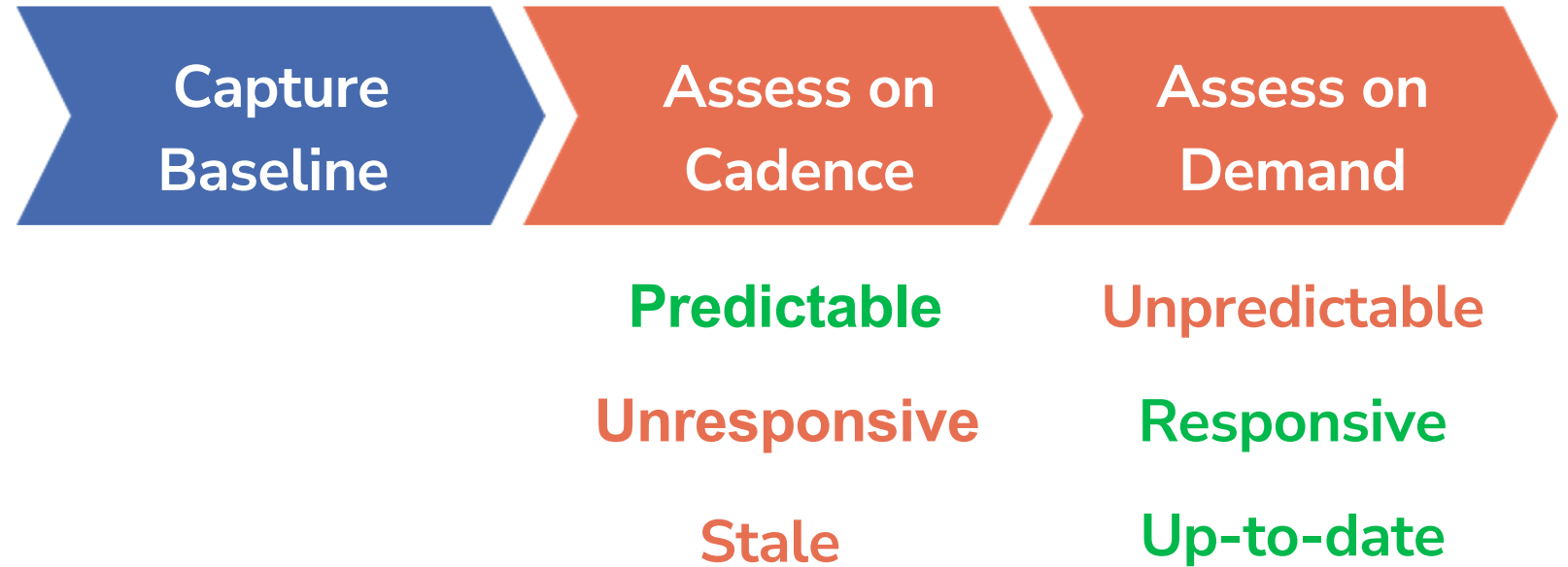
Gen AI Trust [Network](#)  
at [GenAITrust.com](#)



3

Monitor  
vendors for  
changes

The rate of vendor change is accelerating



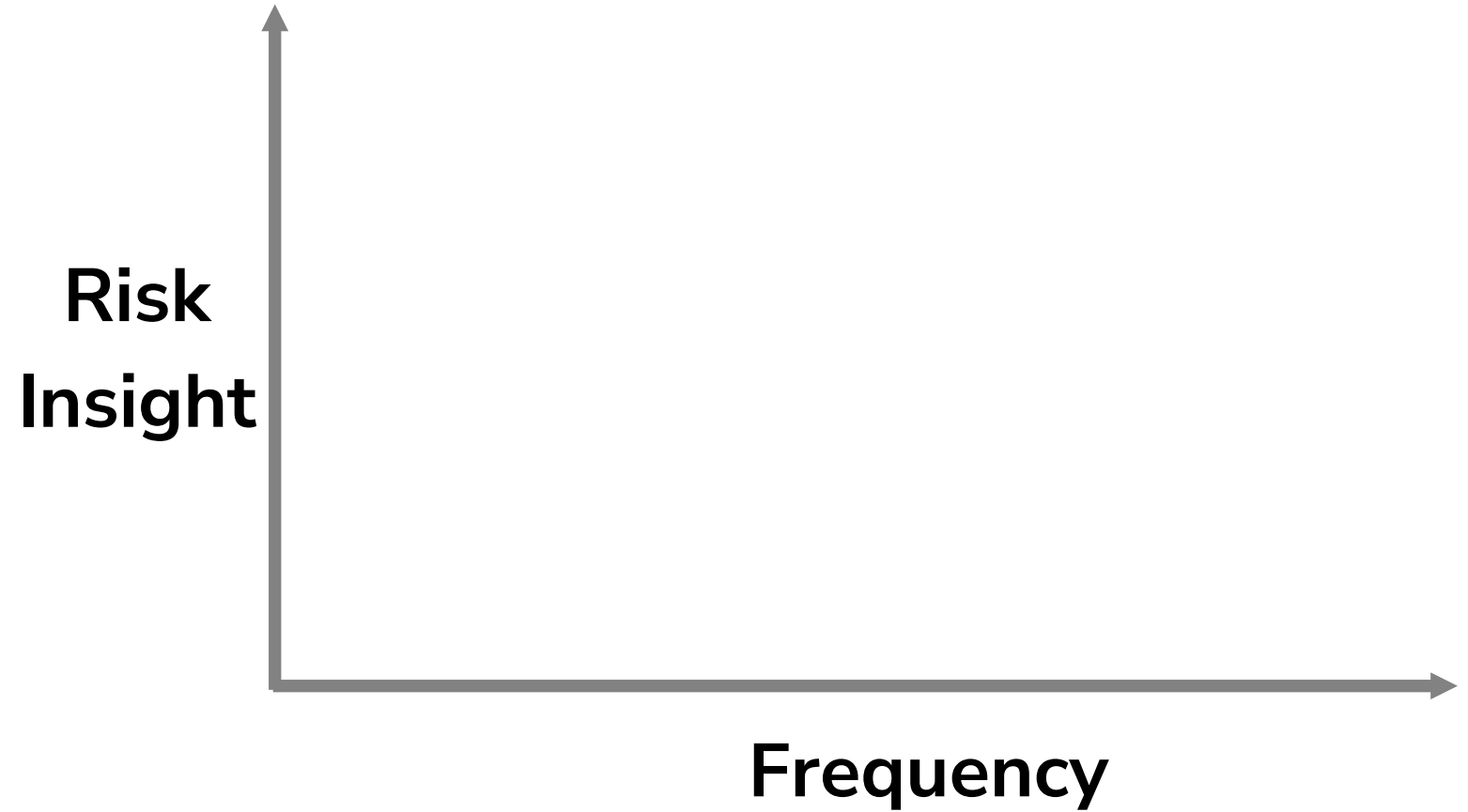




**3**

**Monitor  
vendors for  
changes**

Continuous monitoring of AI risk is hard

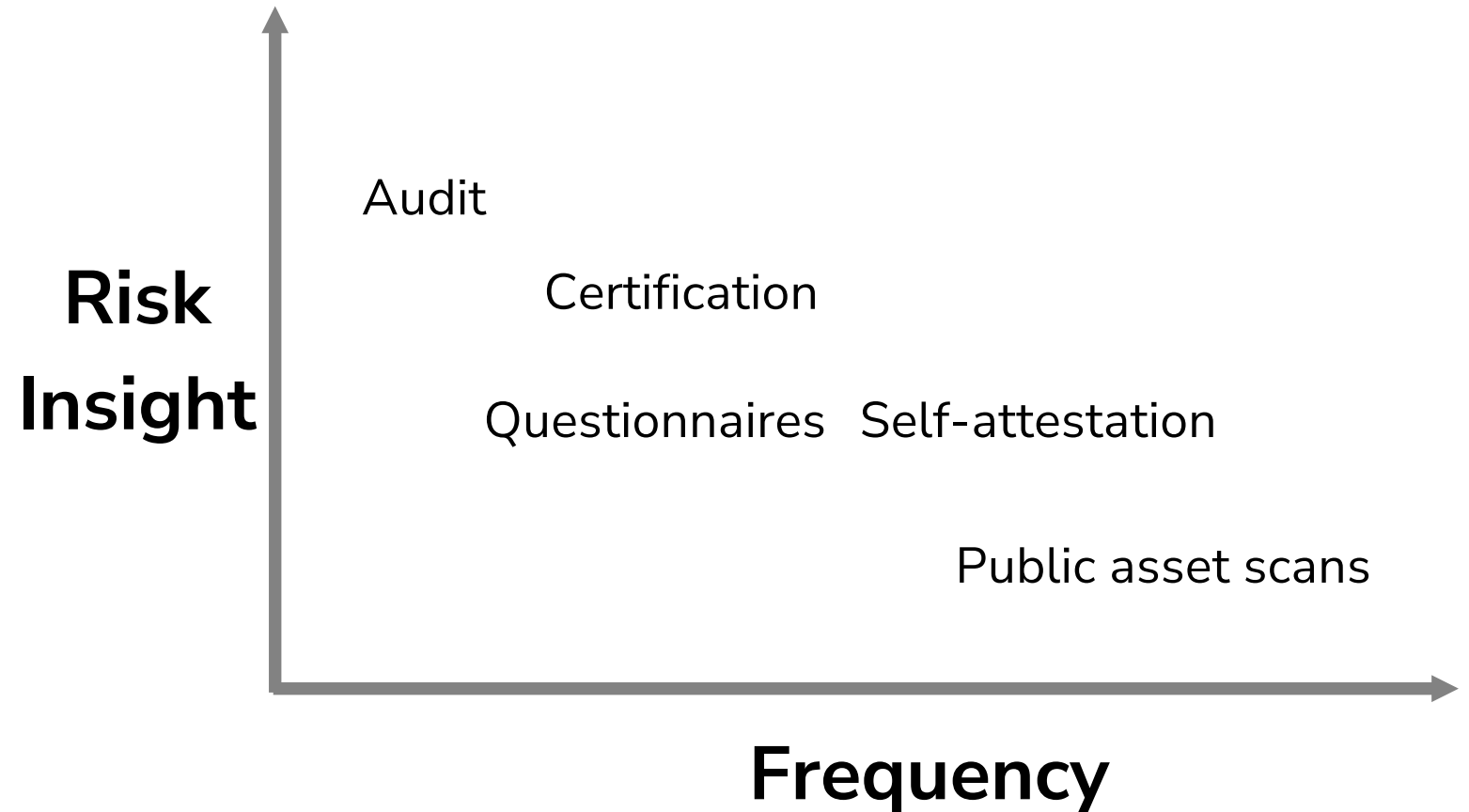




3

Monitor  
vendors for  
changes

## Continuous monitoring of AI risk is hard

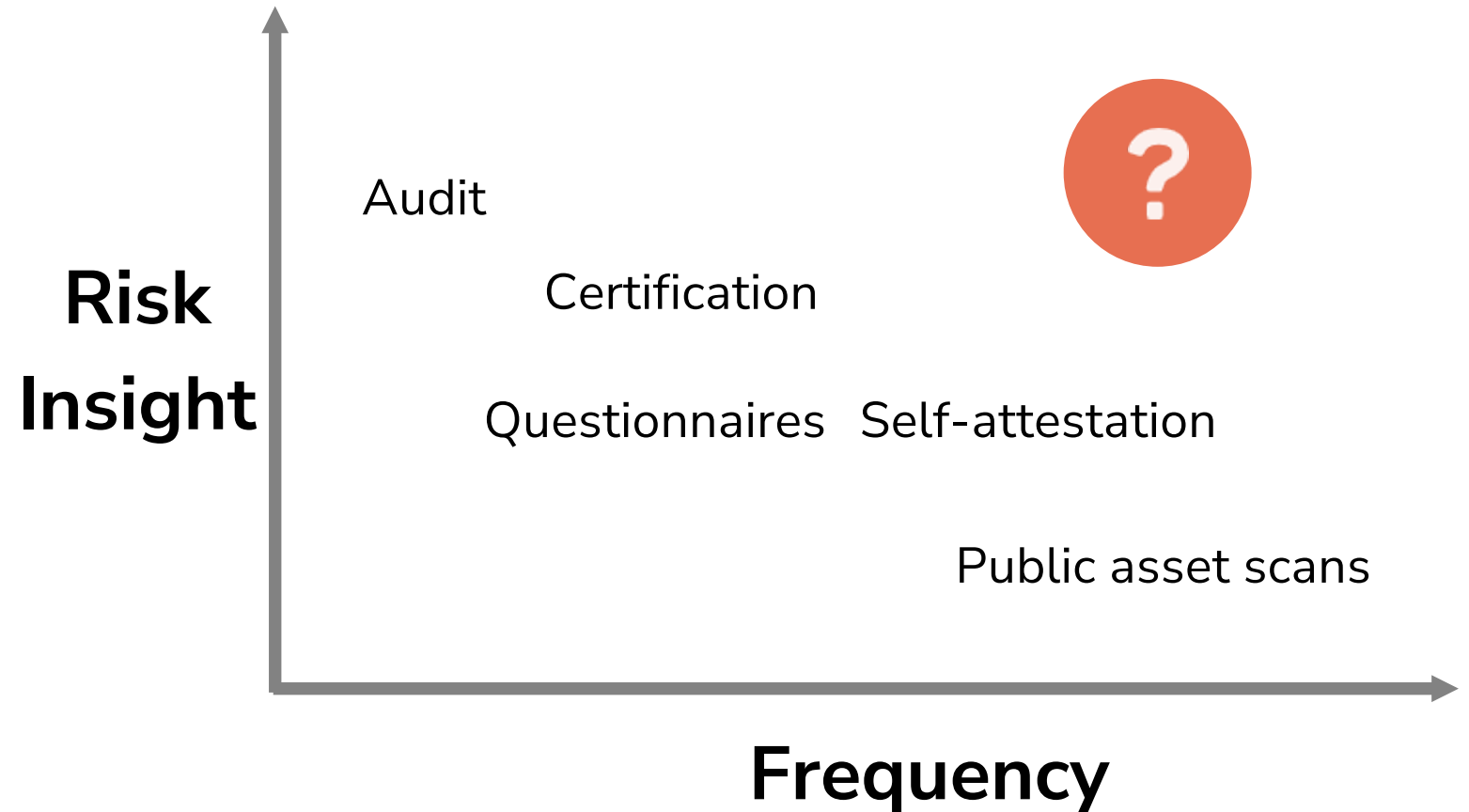




3

Monitor  
vendors for  
changes

# Continuous monitoring of AI risk is hard





3

Monitor  
vendors for  
changes

## Look for high integrity vendors



Transparent AI Disclosures



Accessible Trust Center



Frequent Proactive Updates





**1**

**Align to AI risk frameworks**

**2**

**Build a third party AI inventory**

**3**

**Monitor vendors for changes**



Gen AI Trust [Network](#)  
at **GenAITrust.com**

We set out to understand the challenges  
facing risk leaders in the age of AI.



## We heard:

- ➔ AI risk is complex
- ➔ Standards are evolving
- ➔ User adoption is exploding
- ➔ Vendor risk workflows aren't ready for AI



What we realized is that people want  
**better vendor risk data** so they can  
make **better decisions.**





## Vendor risk data that's:

- Always fresh
- AI-specific
- Integrated
- Verifiable

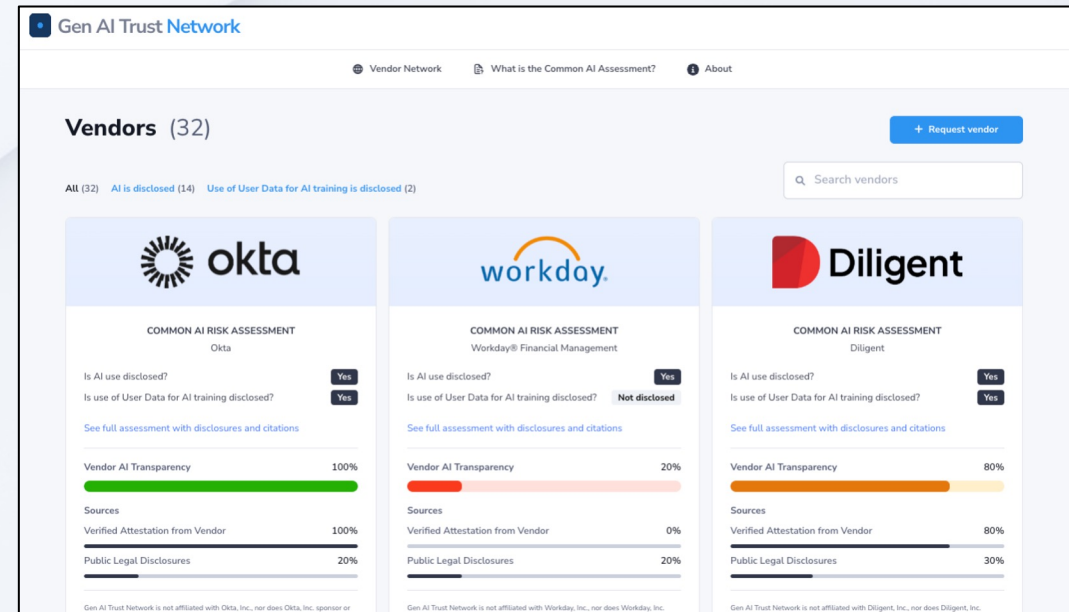


# Real-time risk data is now possible

## Gen AI Trust Network

Vendor risk data that's:

- Always fresh
- AI-specific
- Integrated
- Verifiable



Visit [GenAITrust.com](https://GenAITrust.com) to learn more

# Thank you!



Henry Stanley

Co-founder & CPO

**FABRIK**

Visit [GenAITrust.com](https://GenAITrust.com) to learn more