

# Generative AI for third-party risk management

Discussion paper



# Third party risk management overview

## Context


- 1

The need for efficient operations and risk management puts immense pressure on organizations.
- 2


Increasing efficiency while reducing cost has forced organizations to rely on numerous vendors to meet their business objectives.
- 3

Third parties can include vendors, partners, contractors or service providers that supply materials, software and tools to the organization.


## Types of risks associated with third parties


- 

**Financial risk**  
Third party services impair revenue-generating processes.
- 

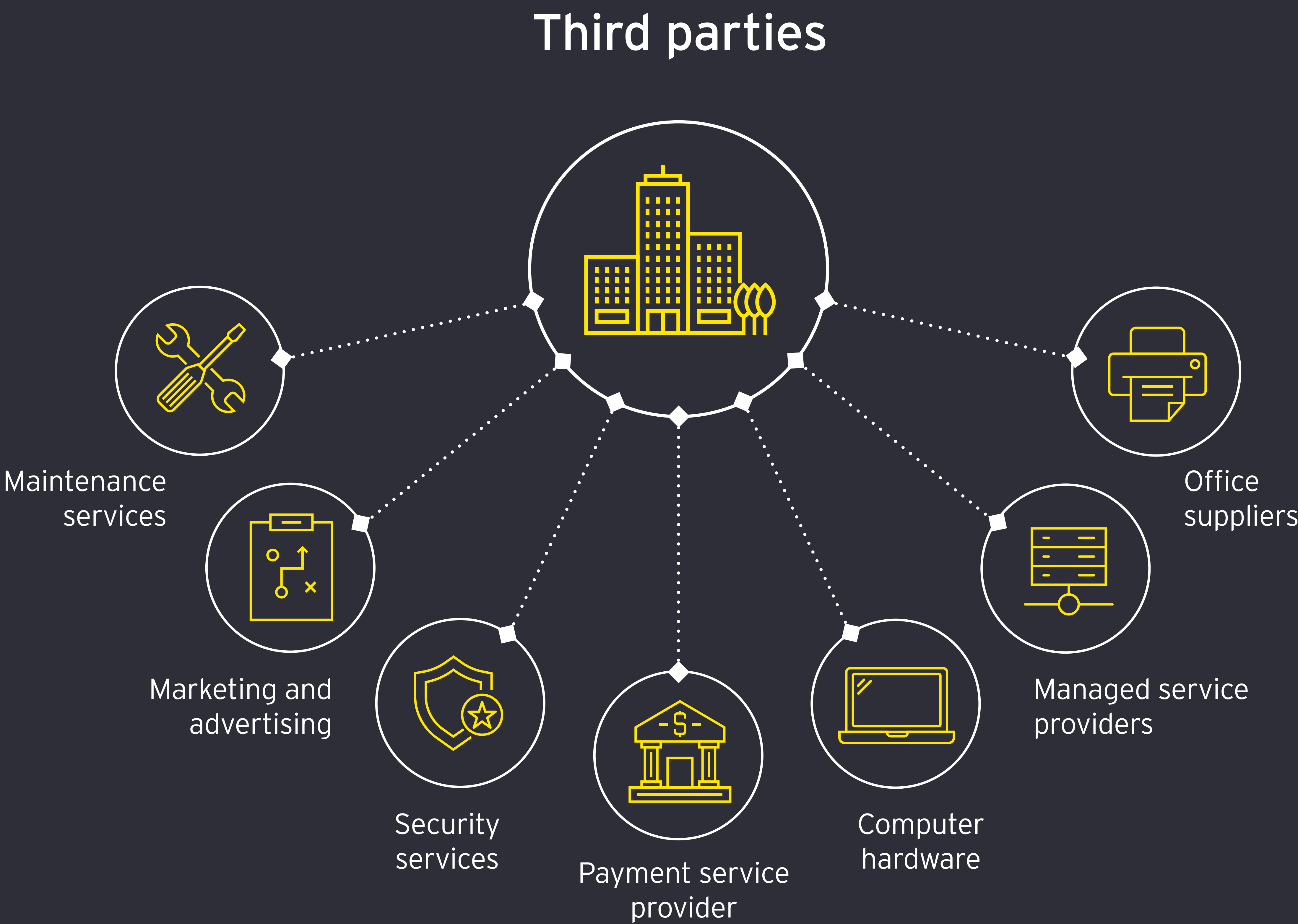
**Reputational risks**  
Third-party relations cause controversy that can negatively impact public opinion.
- 

**Technology/IT risks**  
Third party increases an organization's exposure to cyberattacks, data breaches and disruptions of communications.
- 

**Regulatory/compliance risks**  
Third party fails to comply with laws, regulations and with internal policies.
- 

**Operational risks**  
Third party's poor performance disrupts operations.
- 

**Strategic risks**  
Decisions made by a third party can disrupt an organization's strategic goals.

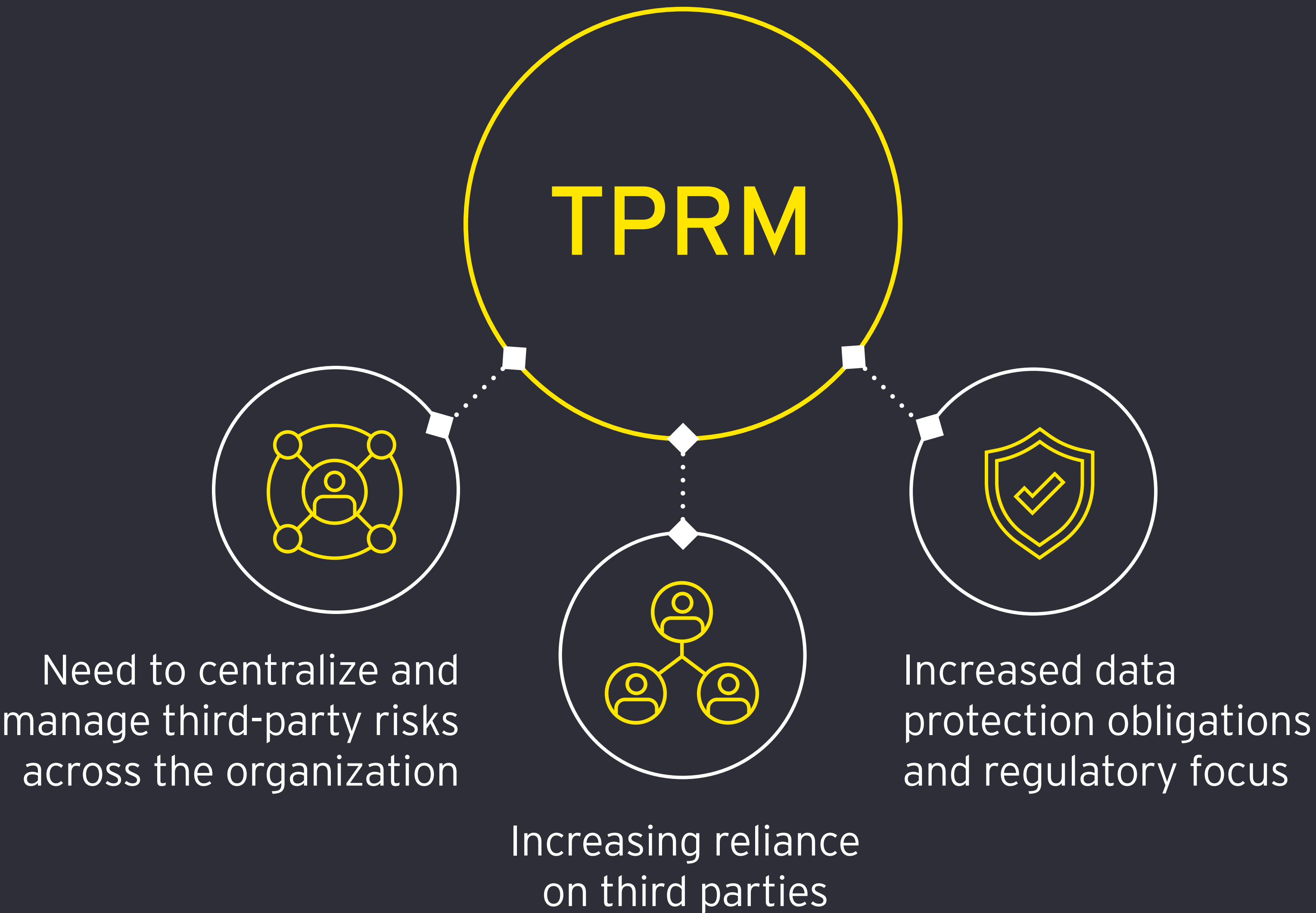




# Third-party risk management trends and themes

Third-party risk management (TPRM) provides a function for management to identify, evaluate, monitor and manage the risks associated with third parties (e.g., third parties/suppliers, intercompany relationships and fourth parties).

## Key drivers for TPRM

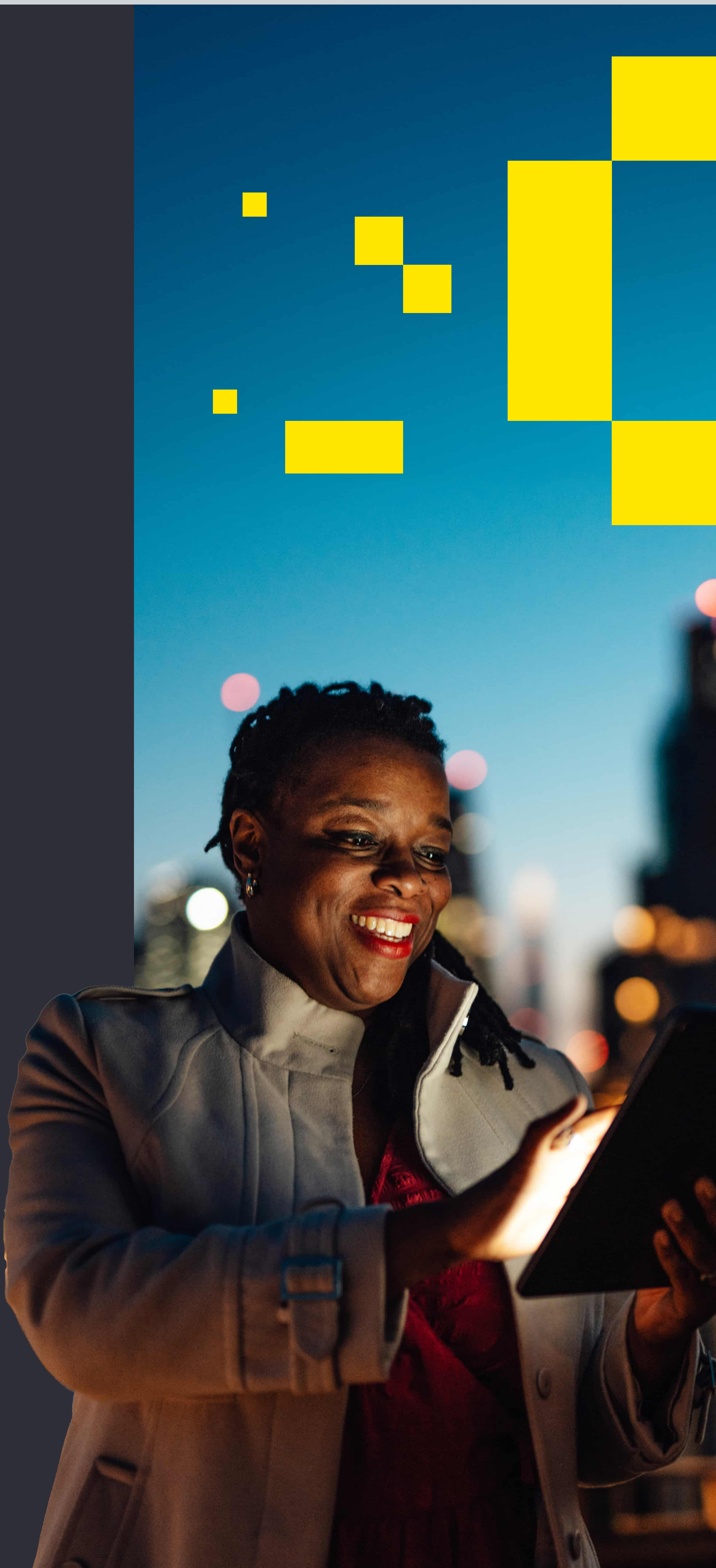


## Benefits of TPRM

- ✓ Proactive management of external risk landscape
- ✓ Strategic enabler
- ✓ Governance of emerging third-party risk
- ✓ Greater risk insights to drive performance

## Industry and regulatory themes for TPRM

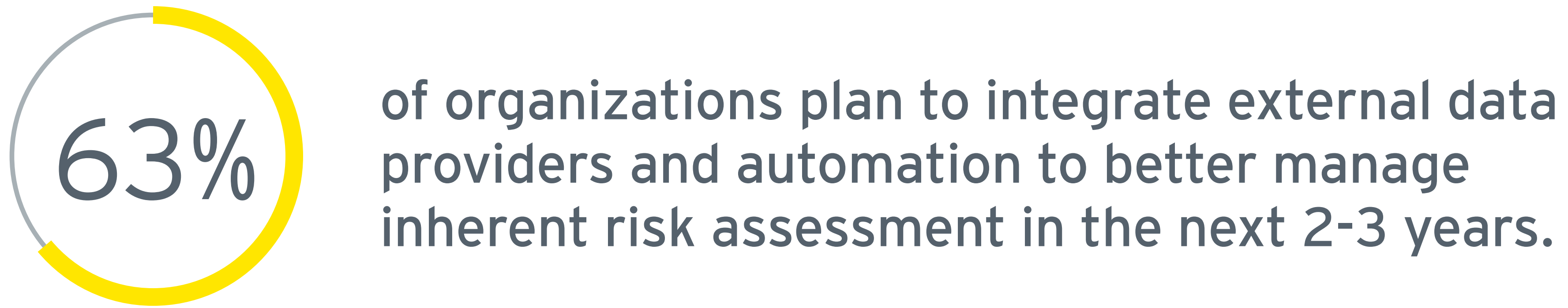
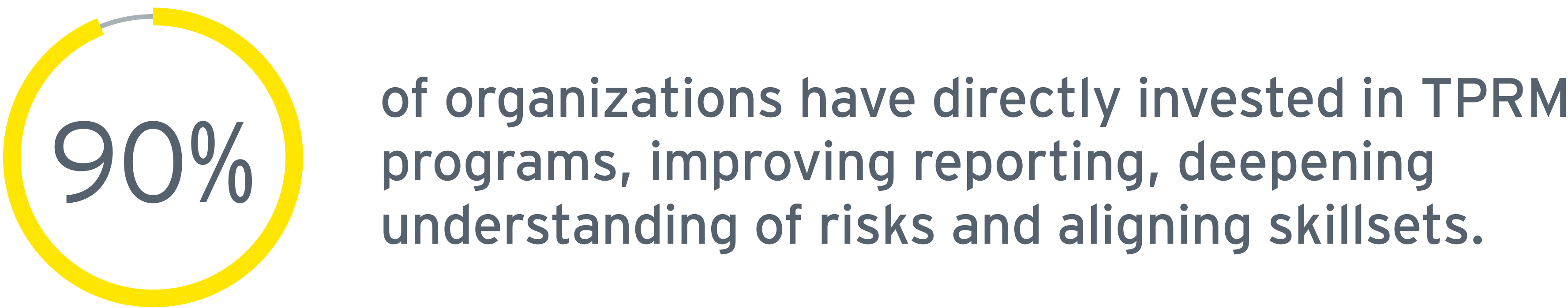
- 1 Third-party population** – Organizations continue to enhance their methodologies to better scope, assess and prioritize risks of third parties.
- 2 Technology** – As investments in TPRM technology platforms continue to rise, integration with other tools has not kept pace, often requiring manual updates to third-party inventories when a new service is added.
- 3 Operating model** – Organizations are developing more centralized organizational structures aligning to the Three Lines of Defense model (3LoD).
- 4 Oversight and governance** – Increased focus on effective third-party risk management reporting provides transparency and accountability, and drives reduced risk while enabling strategic initiatives, driving further reliance on third parties.
- 5 Fourth-party management** – Focus continues on fourth-party risk, with most organizations relying on their third parties to manage/mitigate respective risks.



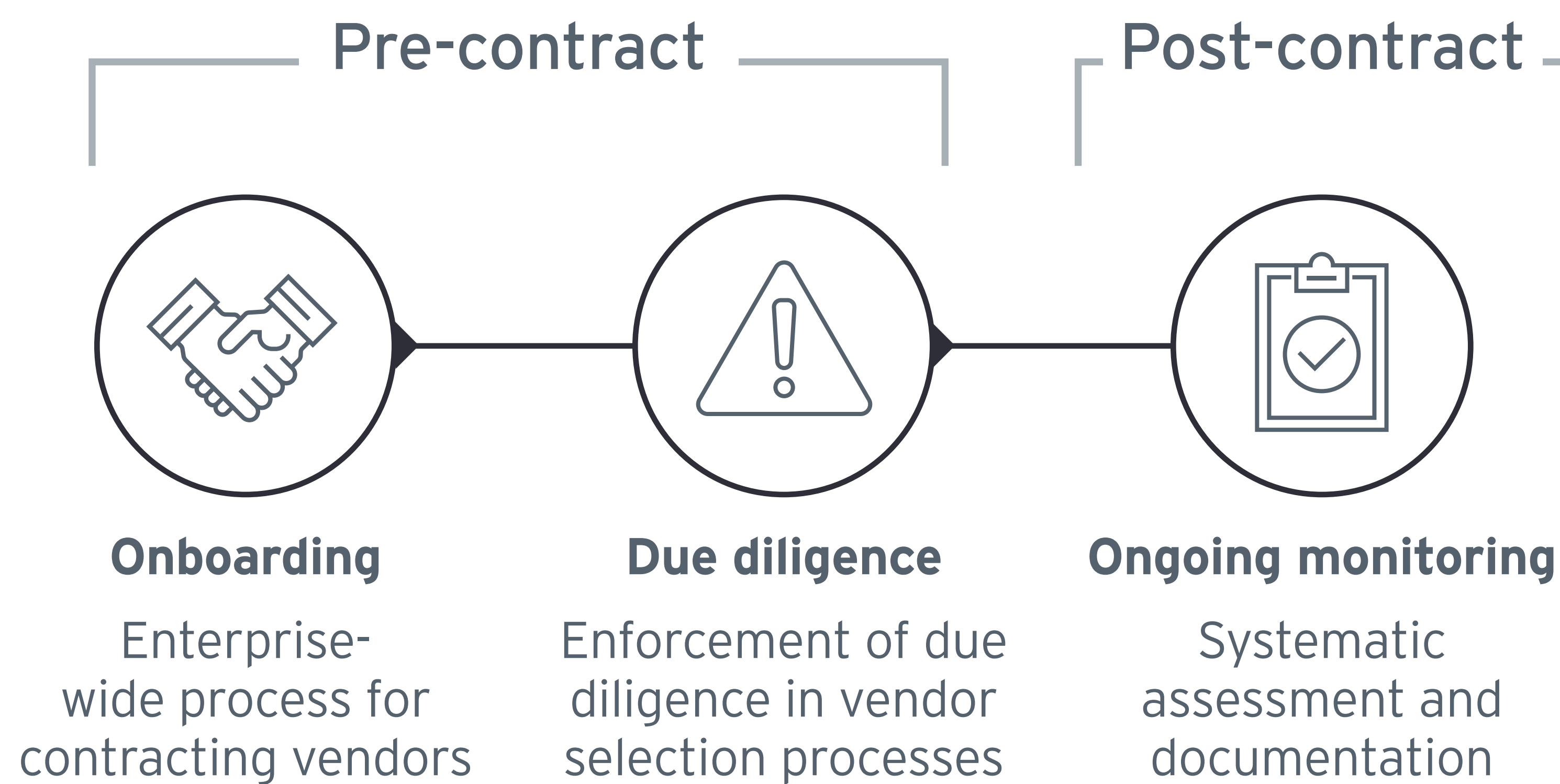


# Adoption and enhancements of TPRM programs

With the backdrop of continuous innovation and evolving regulations, third-party risks have become increasingly prevalent. Therefore, many organizations are re-emphasizing the importance of effective third-party risk management (TPRM).



## Primary components of TPRM lifecycle



A risk-based approach enables organizations to focus on higher-risk third parties and reduce cost/effort associated with lower-risk relationships.

### Risk profiling

Fewer third parties in higher-risk tiers
Organizations are making progress in segmenting risk associated with third parties, focusing on truly high-risk third parties.
More organizations identify critical third parties
Critical third-party listings enable the organization to focus on the critical failure points that demand additional levels of evaluation, reporting and oversight.
Agreement on definition of critical third party
The majority of organizations continue to agree that the potential to impact critical business processes and sensitivity of information involved in providing the service should be used to determine the criticality of third parties.





# AI can increase efficiency and effectiveness in addressing the challenges of TPRM adoption

Adoption of a TPRM program comes with its challenges.

## 1

### Complexity and scope

The assessment of the wide range of risks associated with third parties can be overwhelming, especially for large organizations with complex supply chains. The differentiation between critical and non-critical vendors requires significant effort.

## 2

### Information management

The collection of authentic, accurate and comprehensive data from third parties is a labour-intensive process. The centralization of information obtained from various sources to create a unified view of third-party risk requires significant resources.

## 3

### Integration with existing systems

The compatibility of TPRM tools and platforms with existing IT systems is a key aspects of the TPRM program. The alignment of TPRM processes with the organizations overall risk management framework can pose significant hurdles.

## 4

### Resource allocation

A robust TPRM program requires considerable commitment and resources from the organization, which include investments in technology, tools and personnel.

## 5

### Continuous monitoring

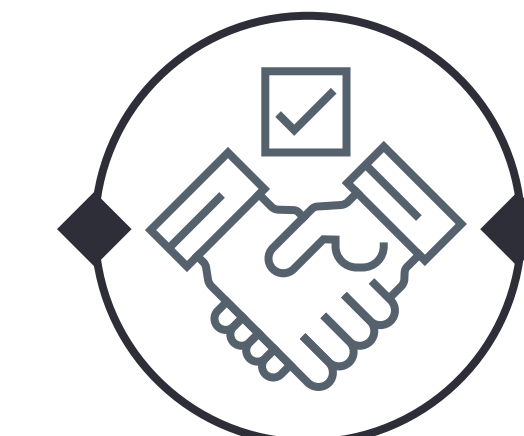
Continuous monitoring is a pillar of any TPRM program. The implementation of ongoing monitoring and periodic reassessment of third-party risk are labour- and time-intensive processes involving long questionnaires.

AI can address the various challenges faced by TPRM programs.



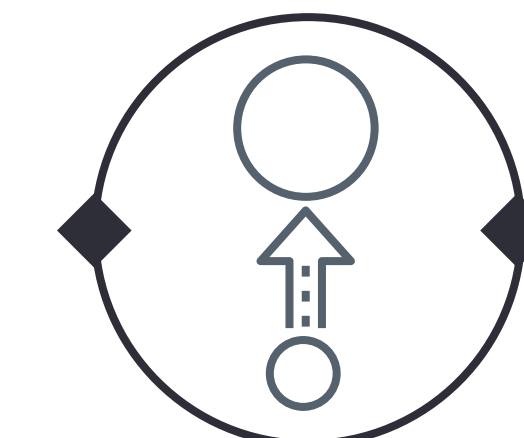
### Handling large amounts of data

AI can handle large amounts of data, ranging from assessment and continuous monitoring to external risk data.



### Greater confidence in decision-making

AI can support and validate decision making processes thereby aiding the risk expert.



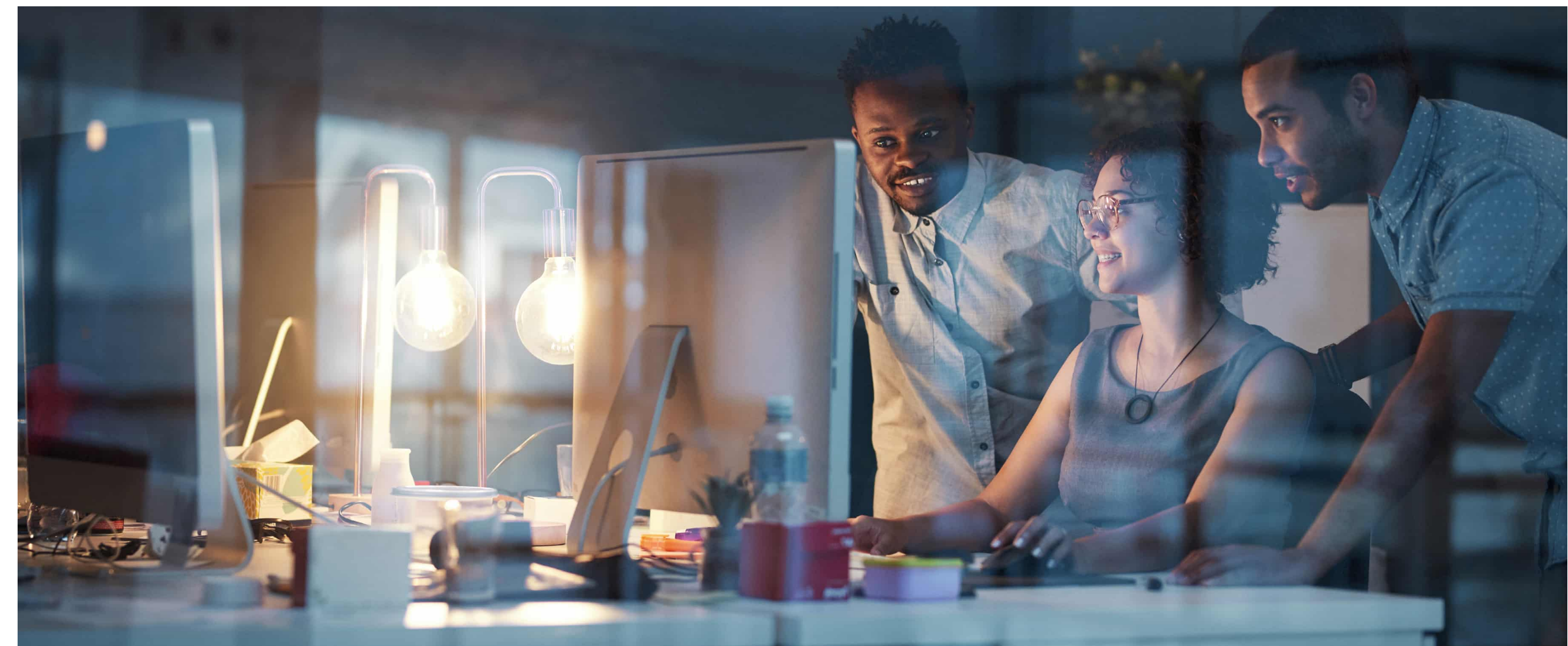
### Scalability

AI can support the growing reliance on third parties and increase efficiency of TPRM teams.



### Aligned with organizational leading practices

AI models can be trained on data specific to the organization, depending on the organization's priorities (e.g., sustainability goals) and risk appetite.





# Role of Generative AI in TPRM

## Deep dive on TPRM lifecycle

An overview of a general TPRM lifecycle is outlined below.

- 1

Intake questionnaire

The intake questionnaire triages the existing third-party inventory to identify vendors that qualify for a detailed inherent risk assessment process, eliminating obvious low-risk vendors.
- 2

Inherent risk assessment

For the vendors that qualify for an inherent risk assessment, the assessment determines the scope and depth of due diligence required.
- 3

Residual third-party risk assessment

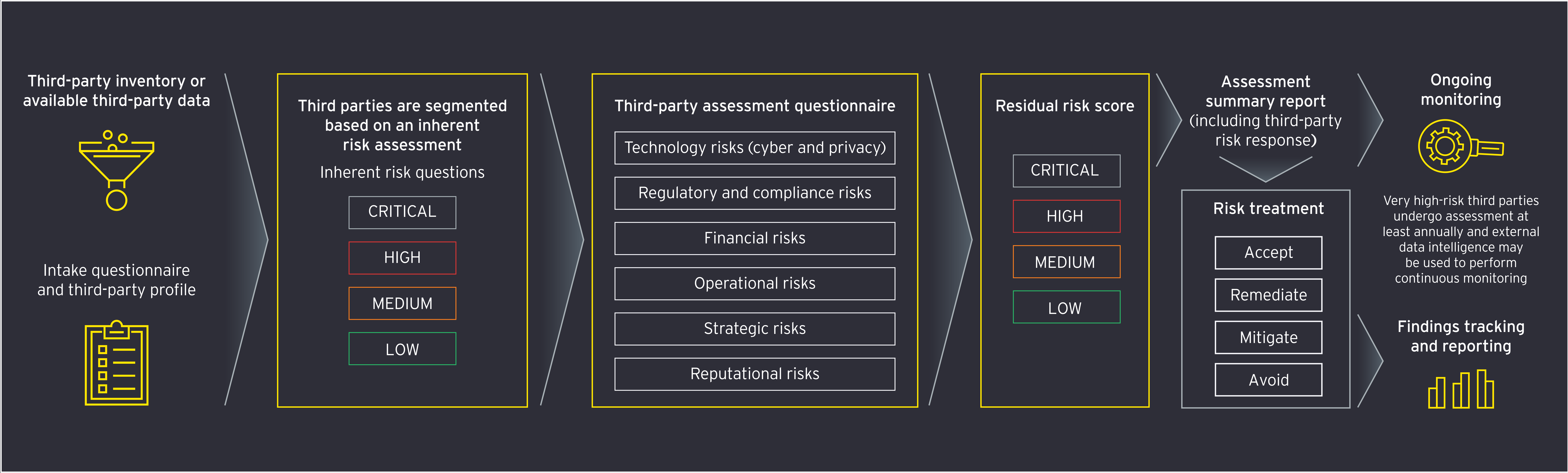
Questionnaires cover prioritized risk areas. They are tailored to the inherent risk rating and nature of the third-party relationship.
- 4

Risk treatment

A residual risk score is assigned to facilitate reporting and risk treatment. Risk treatment is completed prior to contracting with a third party.
- 5

Findings management and monitoring

Findings tracking and reporting is performed until findings are closed. Ongoing monitoring is defined and performed based on the third party's assessed risk.





# Overview of existing approaches in TPRM

Software solutions play a significant role in helping organizations manage the complexities of TRPM by streamlining and automating processes. However, existing processes and technologies pose some limitation in the overall TPRM lifecycle.



**Initial vendor identification and classification**  
Existing technologies allow for identification and classification of vendors by pulling data from a centralized repository.



**Risk assessment**  
Software solutions facilitate comprehensive risk assessments through configurable questionnaires and workflows. Reassessments can be triggered based on previously specified criteria.



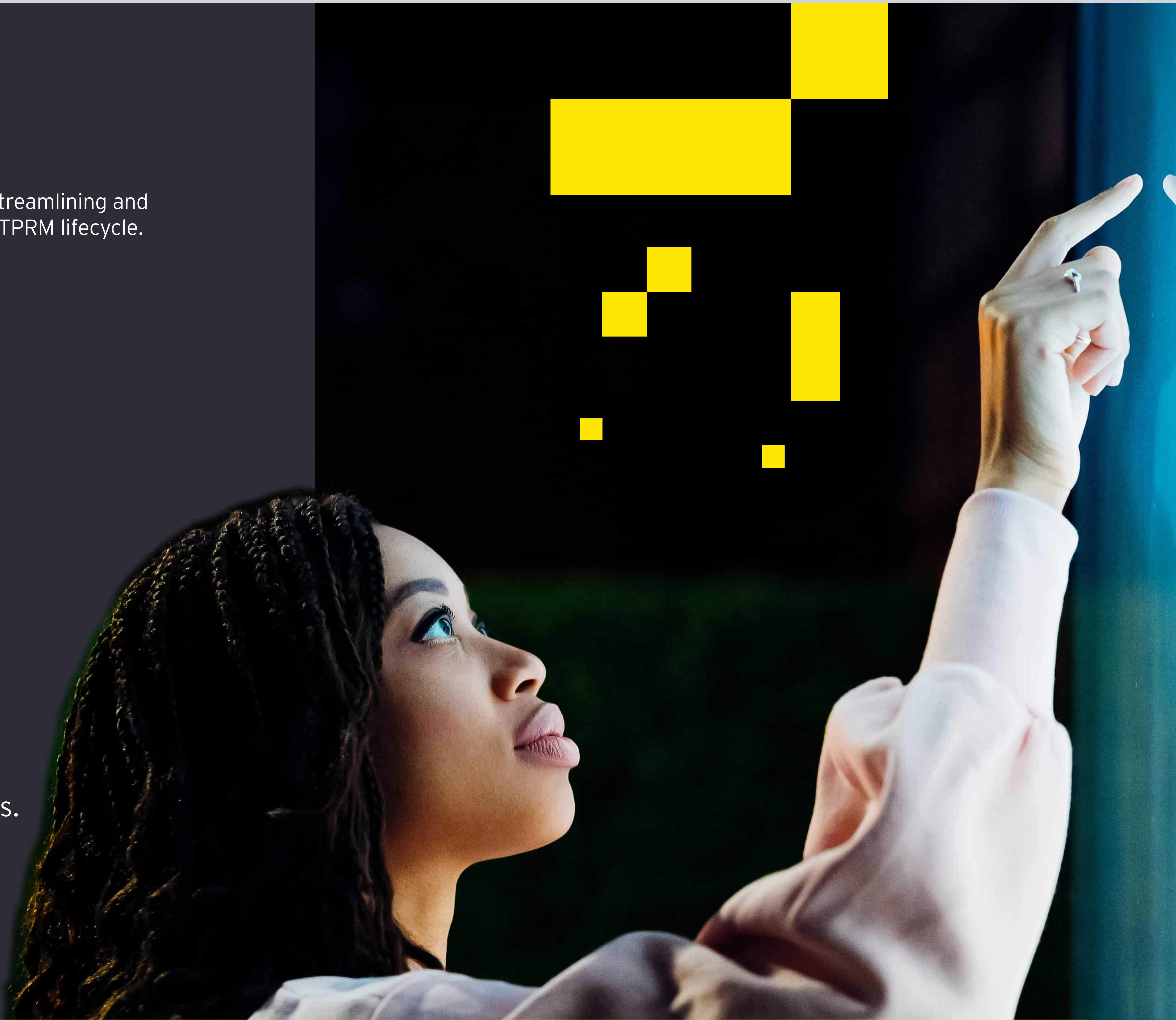
**Due diligence**  
Software solutions manage due diligence processes by automating collection of vendor documentation.



**Contract management**  
Software solutions maintain a repository of vendor contracts in a centralized location. Offer workflows for contract approvals and renewals.



**Ongoing monitoring**  
Software solutions enable continuous monitoring of vendor performance and risk indicators.



## Limitations of existing processes and technologies

1

Platforms can be complex to configure and customize to fit organizational needs. They require time and resources to implement and maintain.

2

Integrating data from various sources and ensuring data consistency can be challenging.

3

Maintaining performance and scalability can become challenging as the number of vendors increases.

4

Manual processes still play a significant role, specifically in data entry, analysis and decision-making.

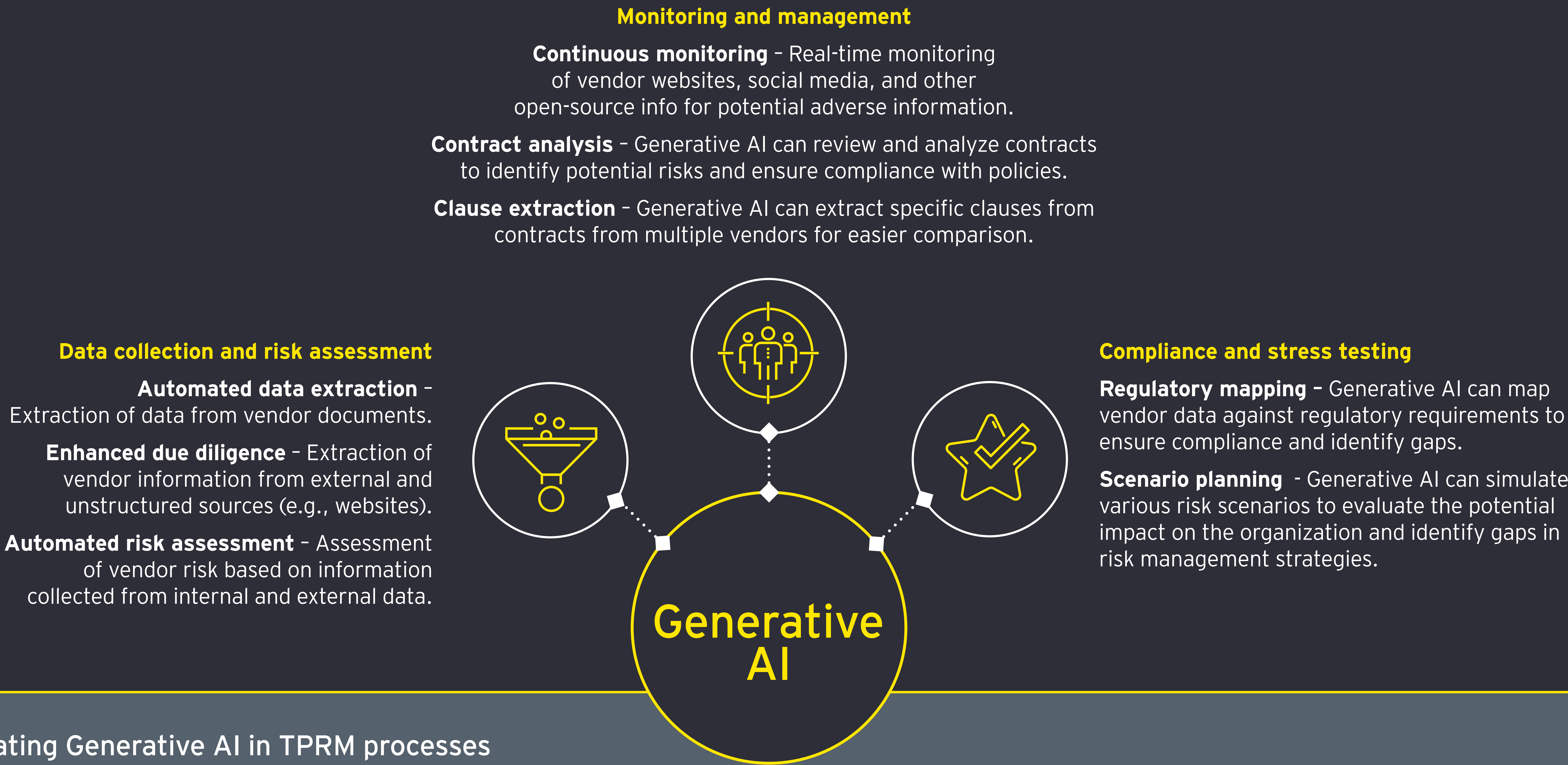
5

Traditional processes and systems have limited predictive capabilities and rely more on analysis from historical data.



# Generative AI can significantly enhance the capabilities of traditional technologies

The capabilities of powerful large language models can enable diverse applications across the third-party risk management lifecycle. A selection of areas of the TPRM program where Generative AI could help are depicted below.



## Benefits of incorporating Generative AI in TPRM processes

1

**Efficiency** – Generative AI facilitates significant improvement in the completion of questionnaires. Vendor processing times can be reduced to minutes.

2

**Scalability** – Generative AI offers a scalable approach to improve the management of a large number of vendors.

3

**Resource optimization** – Prioritization of vendors that require in-depth risk assessment allows for resource allocation where they are most needed, enhancing the overall effectiveness of the risk management program.

4

**Program streamlining** – Streamlining of the third-party risk management program at every stage of the TPRM lifecycle.



# Using Generative AI for enhancing vendor intake assessment

Vendor intake assessment is one of the areas where Generative AI could enhance exiting practices.

## Stakeholders involved for a successful TPRM program



**Internal stakeholders**

Executives  
General counsel  
Board members  
Internal auditors



**External stakeholders**

Vendors  
Regulators



**TPRM implementation**

## Design phase – intake questionnaire

- 1 Development of intake questionnaire
- 2 Development of supporting procedures
- 3 Agreement on the intake process flow
- 4 Validation of the vendor intake approach

## Execution phase



Third-party conflict of interest checks



Search through general ledger and accounts payable data and open-source data to obtain third-party info



Complete intake questionnaire



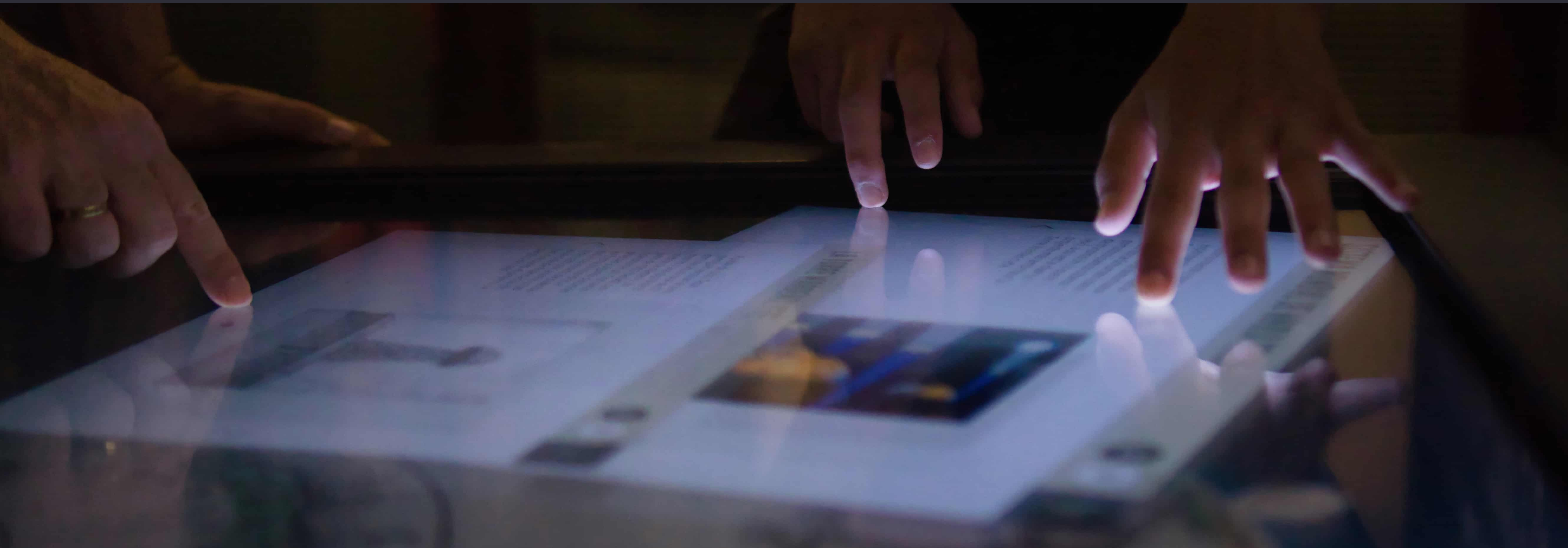
Internal review



Validate with organization



Follow up with stakeholders as needed





# Manual processes create a bottleneck demanding extensive time and effort

## Challenges the intake questionnaire

- 1

The information from the general ledger and accounts payable contains scattered and unstructured data around the nature of the vendor's services to the organization.
- 2

Some organizations have thousands of vendors. A high volume of vendors makes it difficult to complete all intake questionnaires in a timely fashion.
- 3

Lack of a centralized source of data further complicates the processes that enable effective risk profiling.
- ✖

Insights gathered from vendor data are subjected to the assessor's bias, including reliance on a holistic understanding of all available general ledger and accounts payable data.
- ✖

The size of vendor inventory directly affects the time spent in reviewing, gathering and documenting assessment response.
- ✖

Follow-up questions and validation are resource intensive and require greater involvement from the organization's stakeholders.

## Generative AI approach

- 1

Leverage Generative AI to search and retrieve relevant information from internal sources such as general ledger and accounts payable data as well as external sources such as websites.
- 2

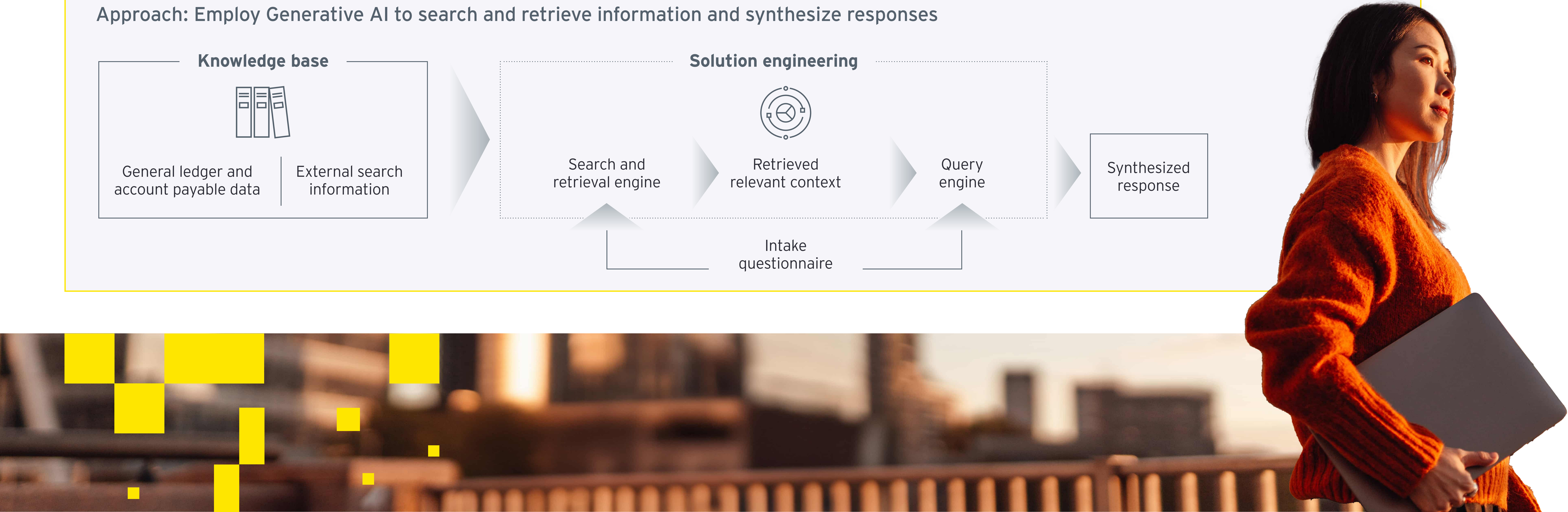
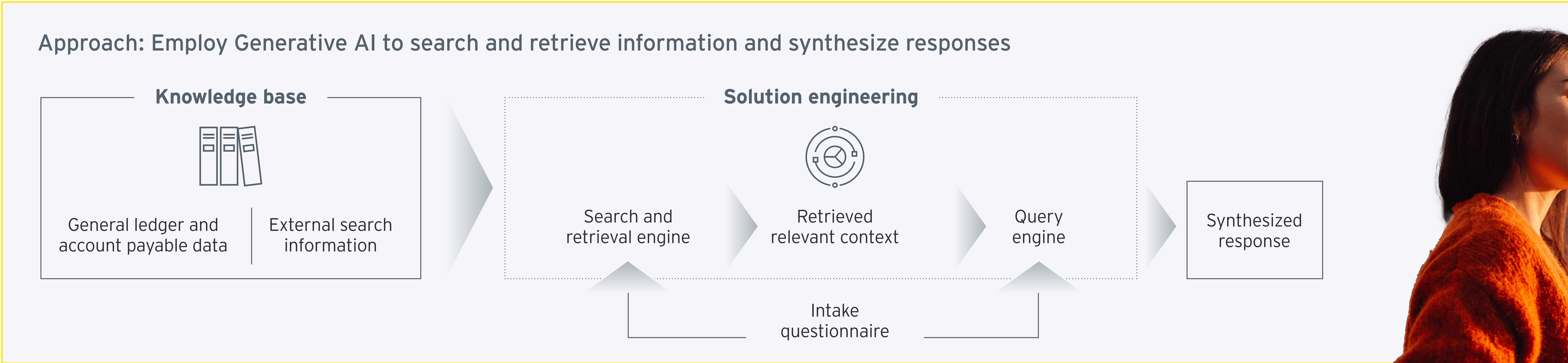
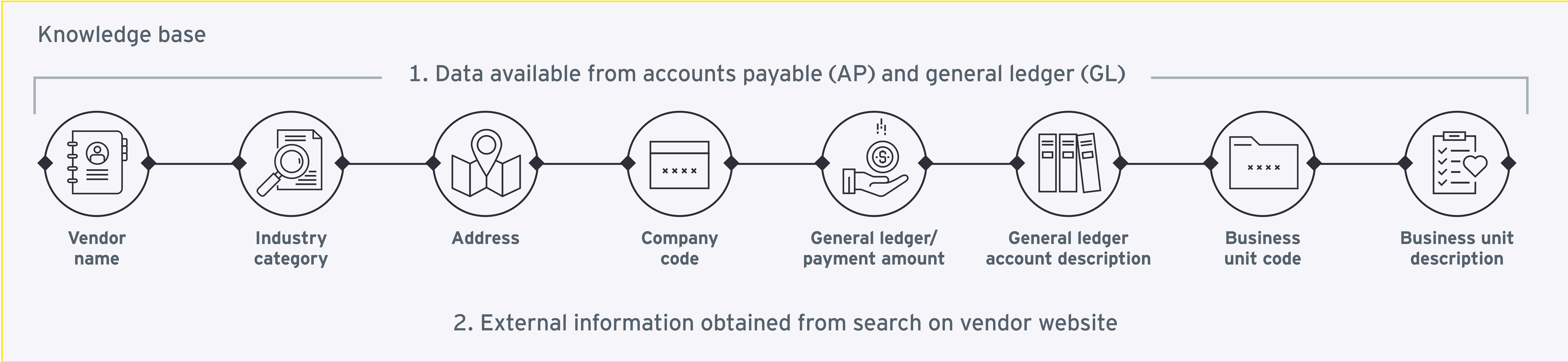
Synthesize responses to the questions in the intake questionnaire.

## Generative AI augmented process





# Generative AI facilitates the completion of vendor intake questionnaires





# Outcome from the Generative AI approach

## Overview of approach

1

Generative AI solution analyzes the information obtained from vendors in inventory.

2

Based on the retrieved information, the Generative AI solution answers eight questions from the vendor intake questionnaire.

3

The responses are analyzed and the Generative AI solution is evaluated for accuracy, processing times and scalability.

## Results

1

Generative AI solution achieved initial model accuracy\* of approximately 80%.

2

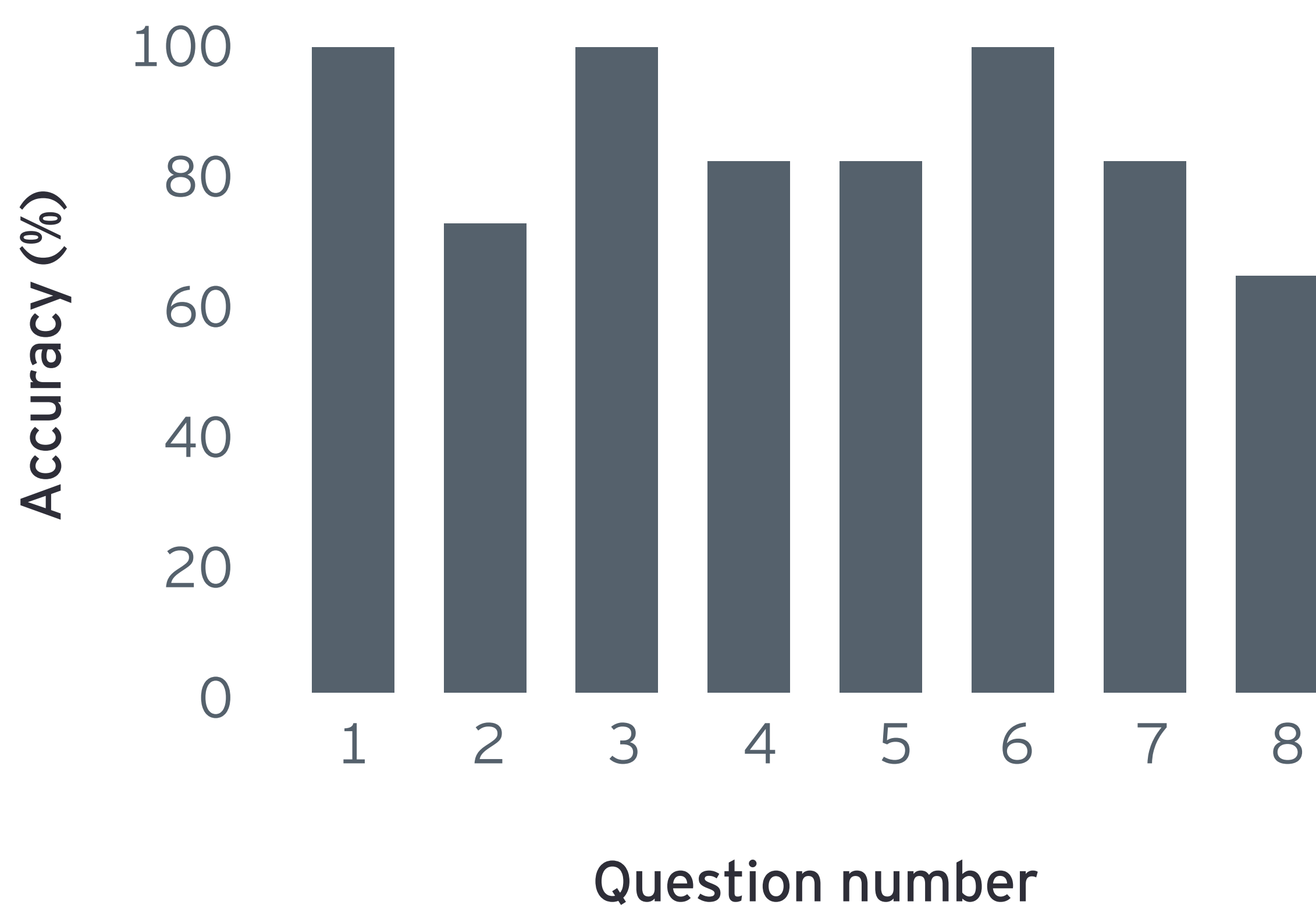
The overall completion time for answering questions reduced to approximately 1 minute per vendor.

3

Processing times of Generative AI solution can be further improved by increasing model usage.

\* Model accuracy refers to the number of correct answers to a specific question out of the total number of answers (number of vendors), expressed as a percentage.

Accuracy of answers to intake questionnaire



## Benefits

✓ Accelerated processing of vendor intake questionnaires

- Generative AI streamlines vendor intake assessment processes by combining human expertise with Generative AI capabilities.
- Generative AI facilitates significant improvement in time required for the completion of intake questionnaires.
- Generative AI provides a highly scalable approach which improves the intake and management of a large number of vendors.

✓ Optimization of resources

- Implementation of Generative AI reduces the manual workload for investigation experts, allowing for higher productivity.
- Generative AI enables the prioritization of vendors that require in depth risk assessment.

✓ Consistency in reporting and documentation

- Generative AI minimizes errors and inconsistencies in documentation by standardizing responses.





# Authors



**Myriam Gafarou**

Partner - Risk Consulting  
myriam.gafarou@ca.ey.com



**Yara Elias**

Senior Manager  
- Risk Consulting  
yara.elias@ca.ey.com



**Jessica Ribeiro**

Senior Manager  
- Risk Consulting  
jessica.ribeiro1@ca.ey.com



**Vishaal Venkatesh**

Manager  
- Risk Consulting  
vishaal.venkatesh@ca.ey.com



**Arnold Zhang**

Senior  
- Risk Consulting  
arnold.zhang@ca.ey.com



**Brian Malile**

Senior  
- Risk Consulting  
brian.malile@ca.ey.com



**Connie Chang**

Senior  
- Risk Consulting  
connie.chang@ca.ey.com





EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via [ey.com/privacy](https://ey.com/privacy). EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit [ey.com](https://ey.com).

© 2024 Ernst & Young LLP. All Rights Reserved.  
A member firm of Ernst & Young Global Limited.

4606305

This publication contains information in summary form, current as of the date of publication, and is intended for general guidance only. It should not be regarded as comprehensive or a substitute for professional advice. Before taking any particular course of action, contact Ernst & Young or another professional advisor to discuss these matters in the context of your particular circumstances. We accept no responsibility for any loss or damage occasioned by your reliance on information contained in this publication.

[ey.com/ca](https://ey.com/ca)