

# Third-Party Risk Management Time to Change: A Modern Approach to Vendor Assessments



# Today's Presenter

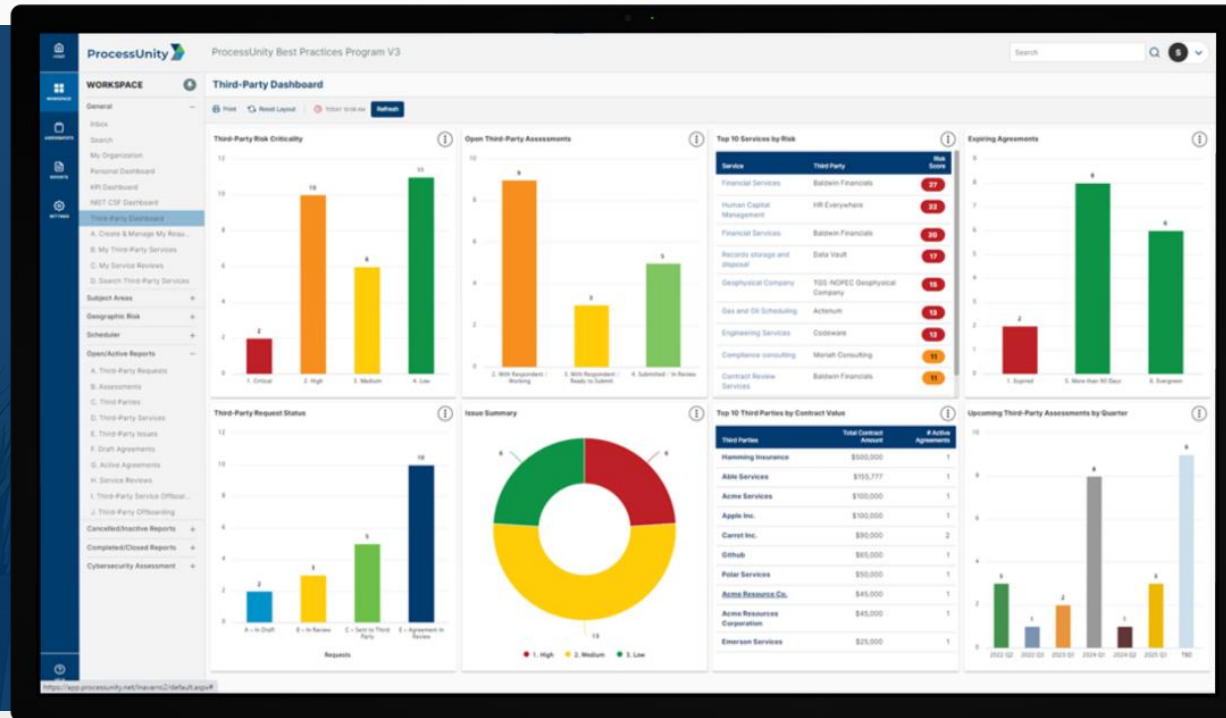


**Ed Thomas**  
Senior Vice President  
ProcessUnity



# The Leader in Third-Party Risk Management Automation

The Top-Rated Third-Party Risk Management Platform



The Most Successful Customer Implementations in the Market



Out-of-the-box best practices program



Unparalleled subject matter expertise



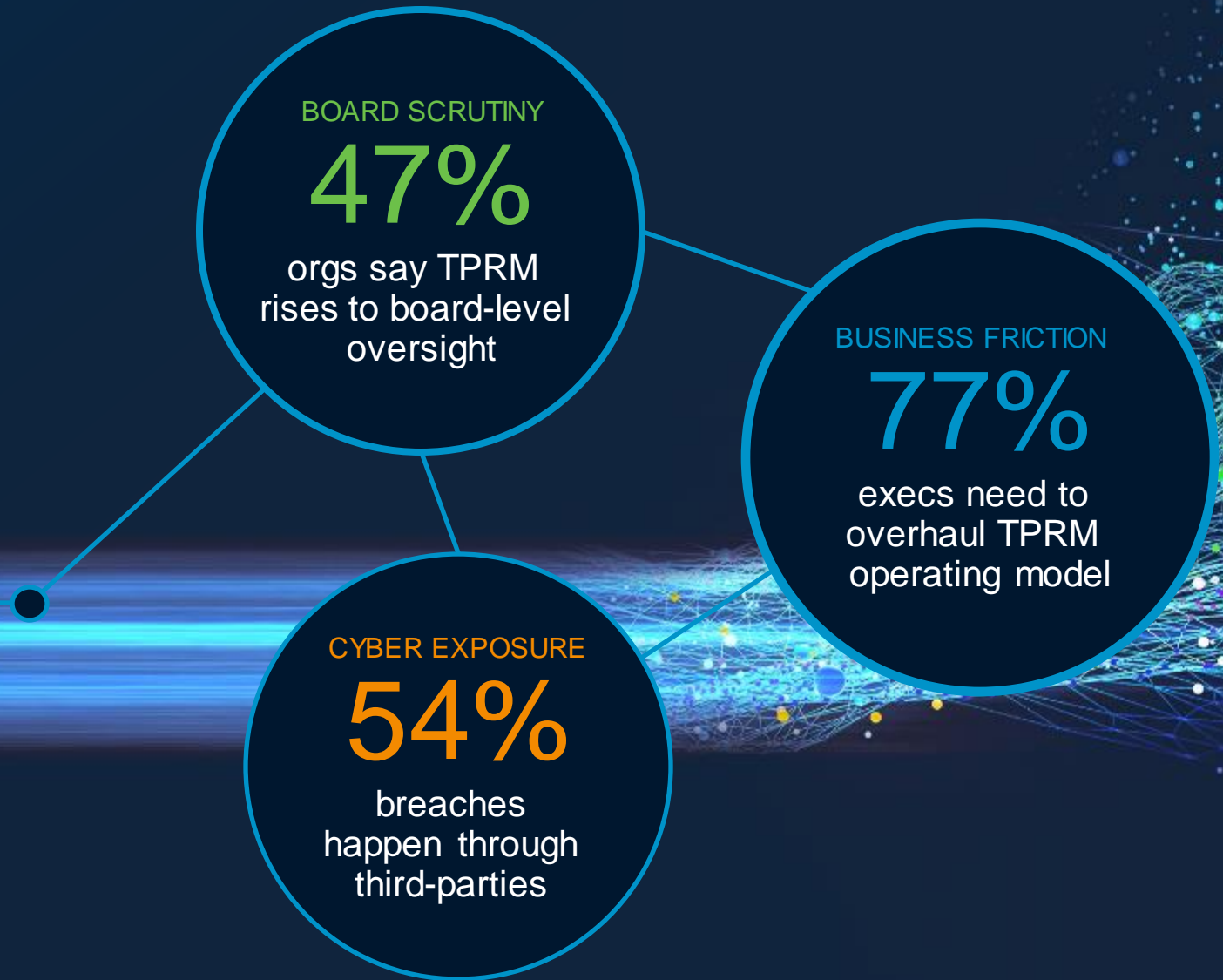
The shortest implementation times

# Today's Agenda

- The Third-Party Risk Vulnerability Gap
- Thinking Differently
- Critical Components for Mature TPRM
- The Assessment Process Reimagined
- Summary / Q&A



# Third-party risk has reached a **tipping point**



Sources: Deloitte, Venture Beat, KPMG



# TPRM Tipping Point

## FORRESTER®

According to Forrester\*, 69% of risk decision-makers identified their TPRM program as manual. **“Even more concerning: Just 30% indicated that their organization’s TPRM program evaluates at least half of its existing third-party relationships.”**

(\*Forrester, The Third-Party Risk Management Platforms Landscape, Q4 2023)

# TPRM demands **outpace** resources



**Explosion of  
third-parties**



**Third-party Risk  
Vulnerability Gap**

Slow | Limited coverage |  
High friction | More exposure

TPRM Resources

YOUR VULNERABILITY GAP

# What Makes Up **Your** Gap?

Onboarding  
Cycle Times

Assessment  
Backlog

Lack of  
Vendor  
Tiering /  
Prioritization

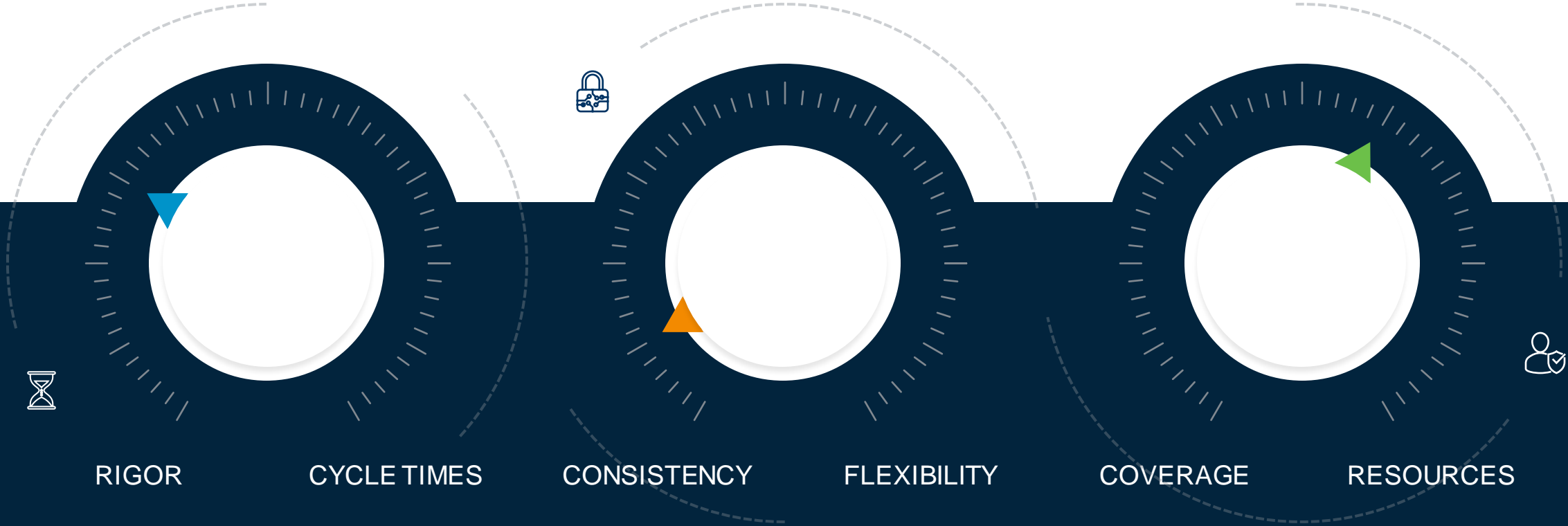
Emerging  
Vulnerability  
Attack  
Response

Inadequate  
Portfolio  
Coverage

Hard-to-  
Assess  
Vendors



# You are stuck in a **no-win** balancing act



We need **to think differently**

**What's needed is a  
TPRM Force Multiplier**

Modernize programs



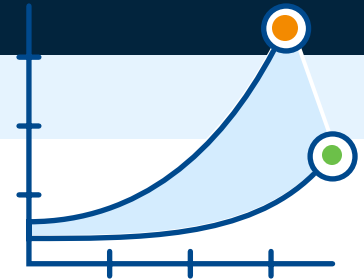
Eliminate tradeoffs



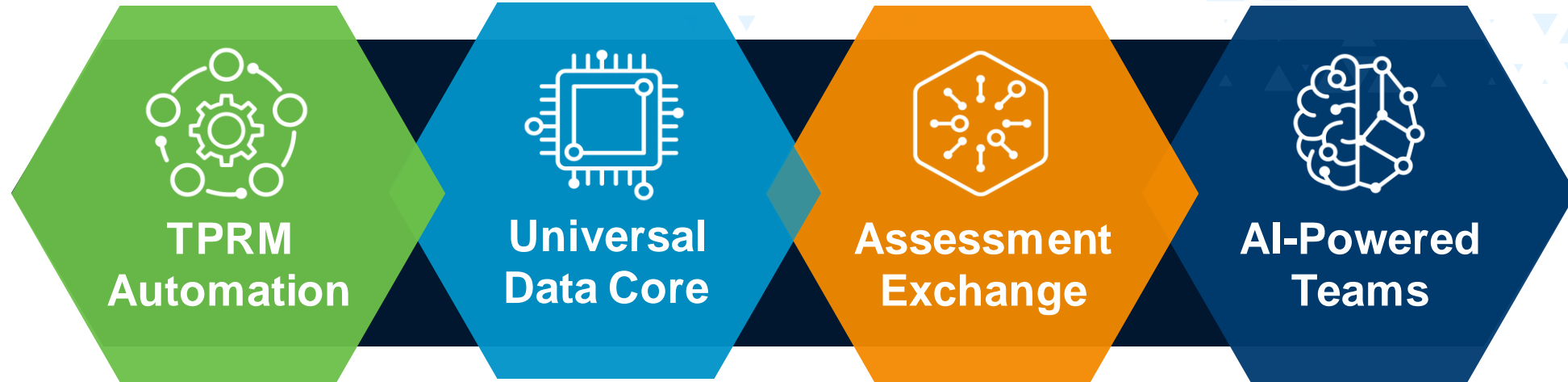
Elevate teams



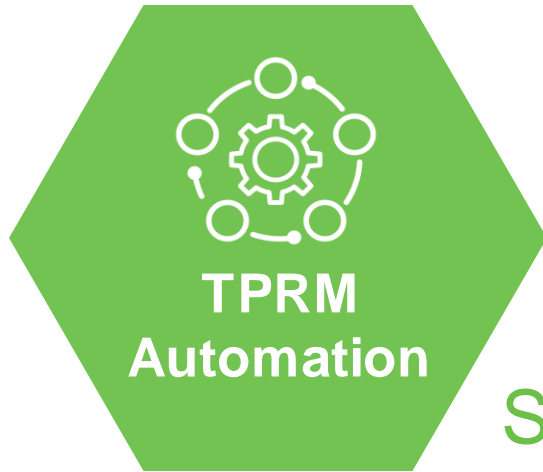
Close the gap



# TPRM Foundational Components

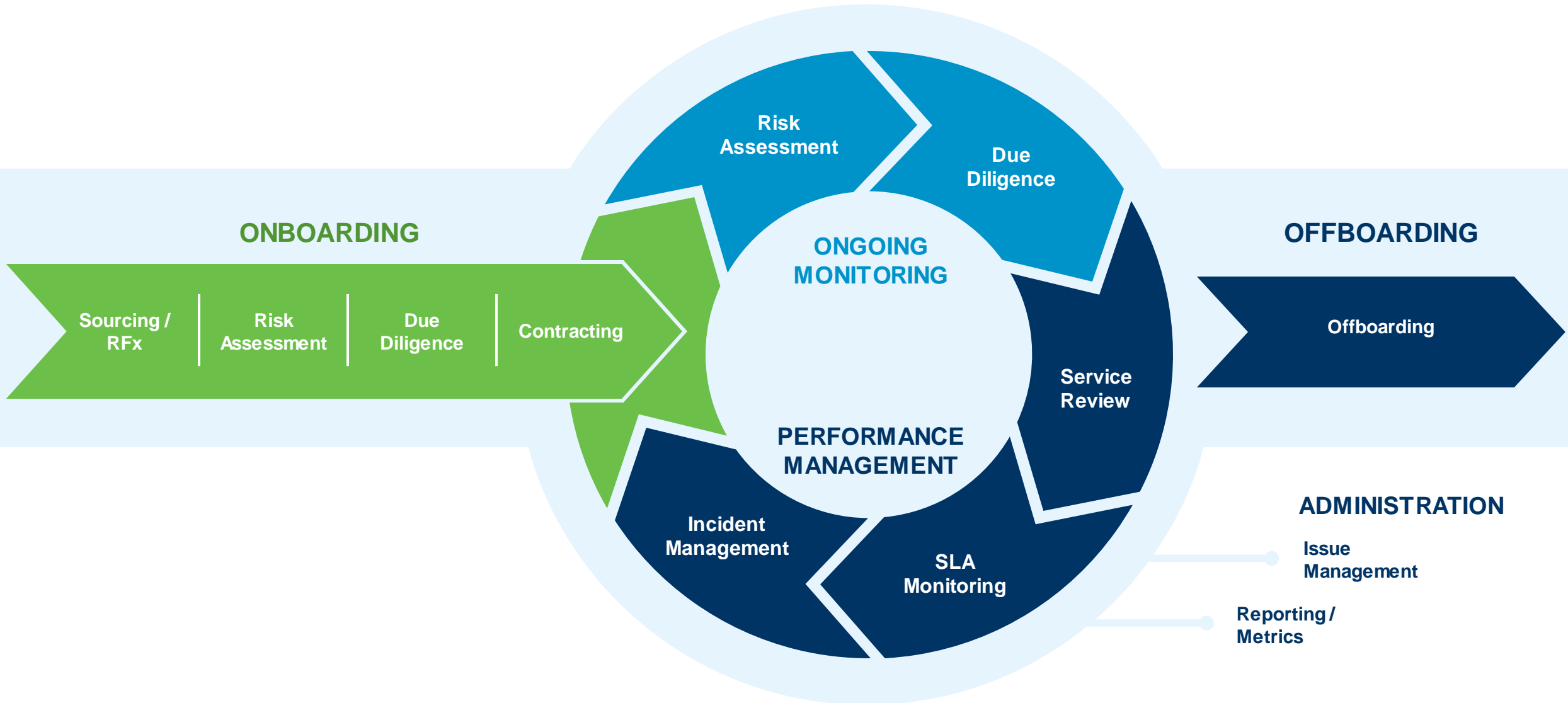


The Force Multiplier Comes from the Four  
Critical Components for Modern TPRM



Streamline TPRM Processes with Automation.

# Automate the Third-Party Risk Management Lifecycle





# Automation: What to Look For



TPQM  
Processes



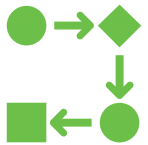
Assessment  
Engine



Vendor  
Portal



Scoring  
Systems



Workflow



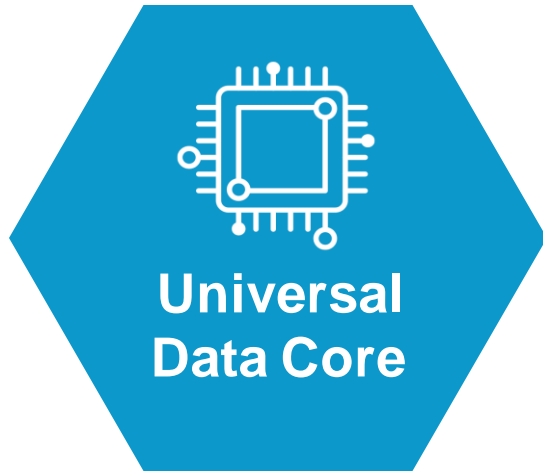
Configuration



Integrations



Reporting



Third-Party Risk is a Data Problem.  
Solve it with a Universal Data Core.

# Third-Party Risk is a Data Problem

200

Assessments

X

200

Questions Per Assessment

---

40,000

Items to Be Reviewed

# Third-Party Risk is a Data Problem

$$\begin{array}{r} 200 \\ \times 200 \\ \hline 40,000 \end{array} +$$

- Vendor Profiles
- Policies & Procedures
- Findings
- Issues Management
- Communications
- Ratings / Scores
- Contracts
- RFPs
- Performance Reviews
- SLAs & Metrics
- Reports

# Third-Party Risk is a Data Problem



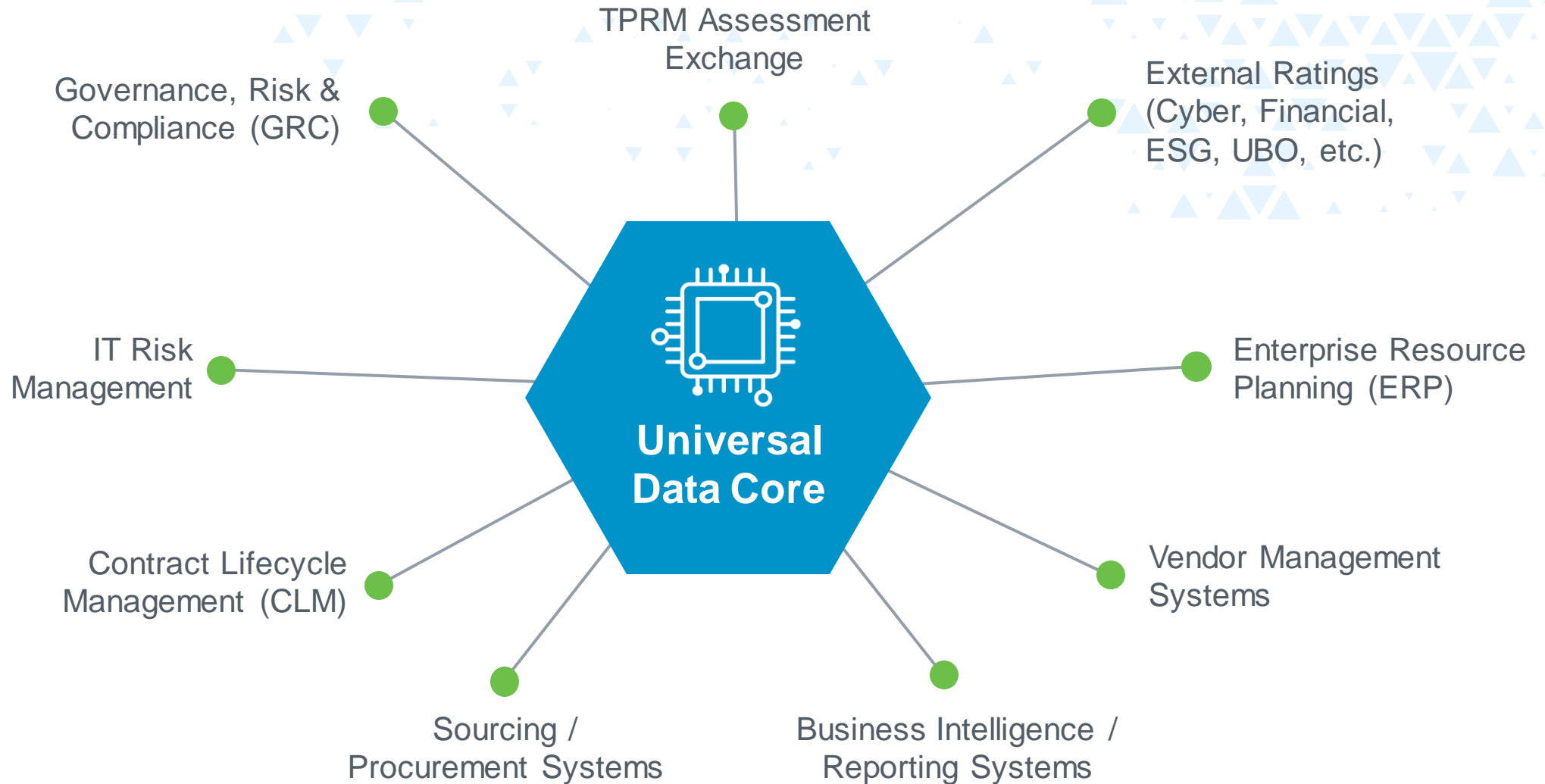
**WHERE DOES ALL  
THIS DATA LIVE?**



**HOW DO WE  
REPORT ON IT?**



# A Single System of Record for TPRM





## Assessment Exchange

Tap into a Library of Completed Assessments.

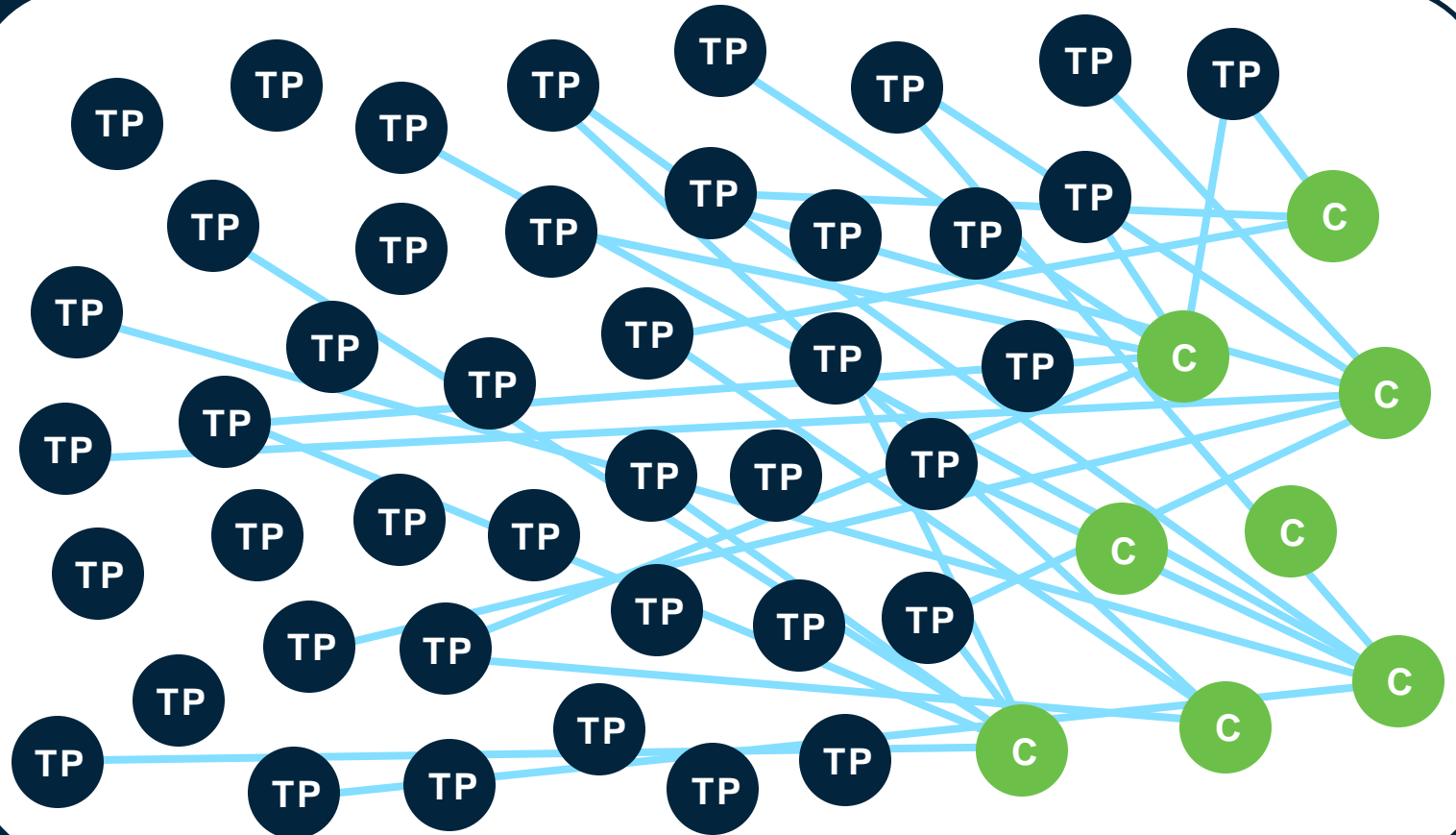
# Assessment Exchange

**ASSESS ONCE / SHARE  
MANY MODEL**

**COMPLETED, ATTESTED &  
VALIDATED ASSESSMENTS**

**ASSESSMENTS FOR  
LARGE THIRD PARTIES**

**ANALYTICS BASED ON  
LARGE DATA SETS**



# Assessment Exchange: What to Look For



Hard-to-Assess  
Third Parties



Portfolio  
Coverage



Data Refresh  
Rate



Assessment  
Validation



## AI-Powered Teams

Elevate Human Performance.



# AI-Powered Teams Elevate Human Performance

FREE YOUR TEAM FROM ROUTINE TASKS, FIND PATTERNS IN LARGE DATA SETS

**CRITICAL**

**HIGH**

**MEDIUM**

**LOW**

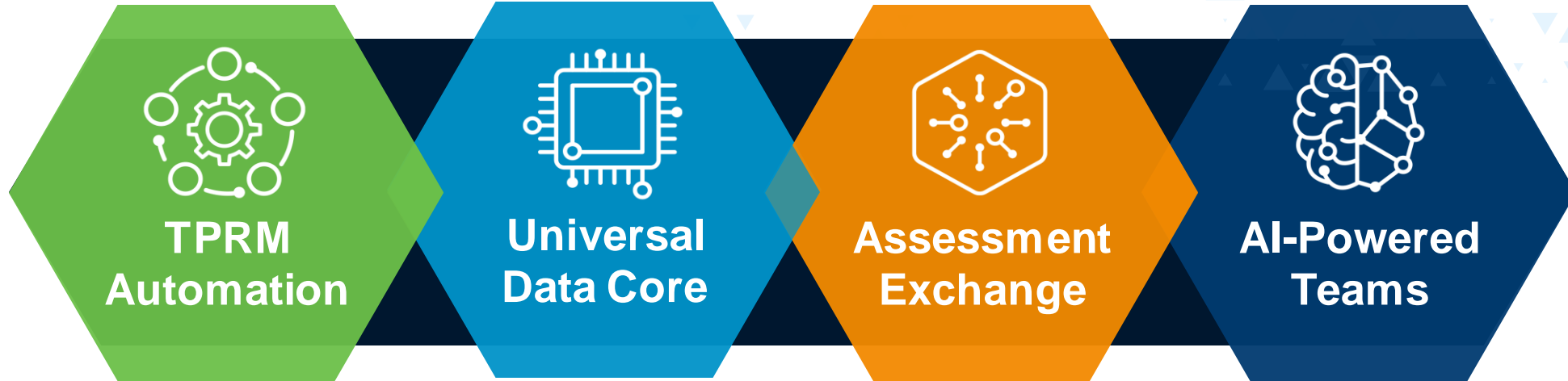
Identify & Prioritize  
Third-Parties

Expose Hidden Risks  
with Predictive Insights

Rating: **Good**

**85** / 100

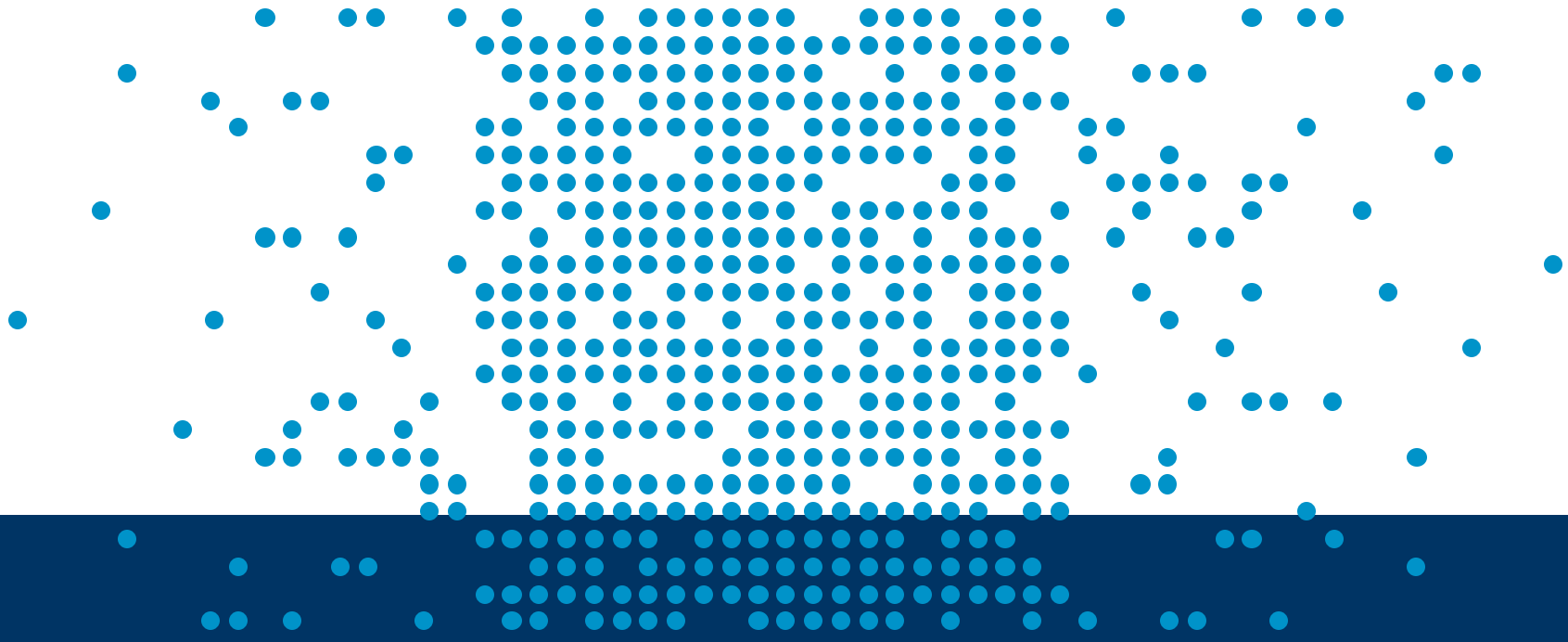
Accelerate Vendor  
Policy Reviews



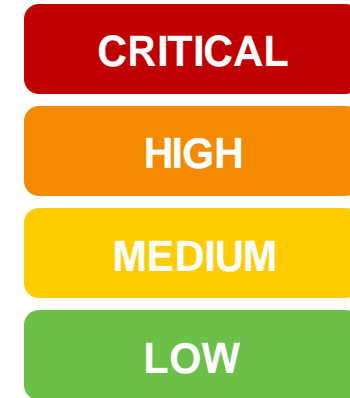
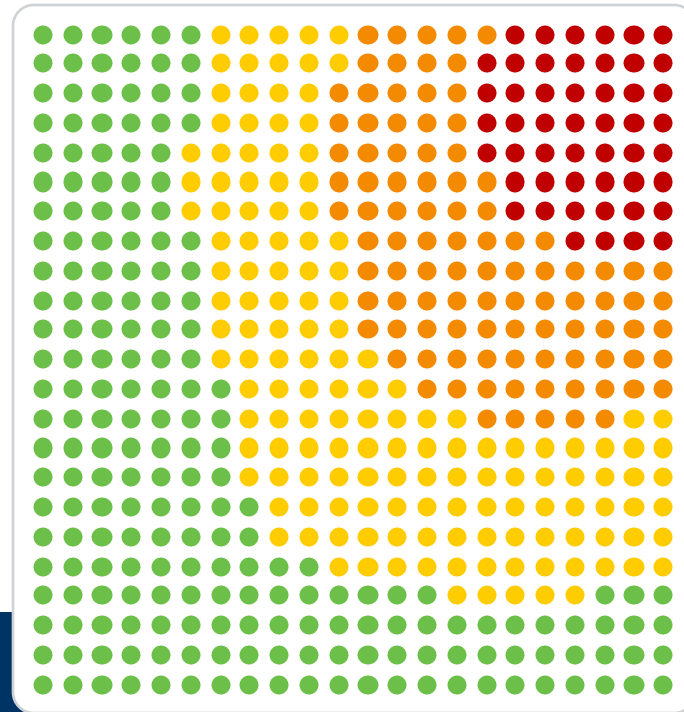
Together, These Components Change  
How We Assess Third Parties

STEP ONE

# Tier / Classify Your Vendors via Inherent Risk



# Your **Third-Party** Ecosystem



Prioritized by **Inherent Risk**

# Option 1: Inherent Risk Questionnaire

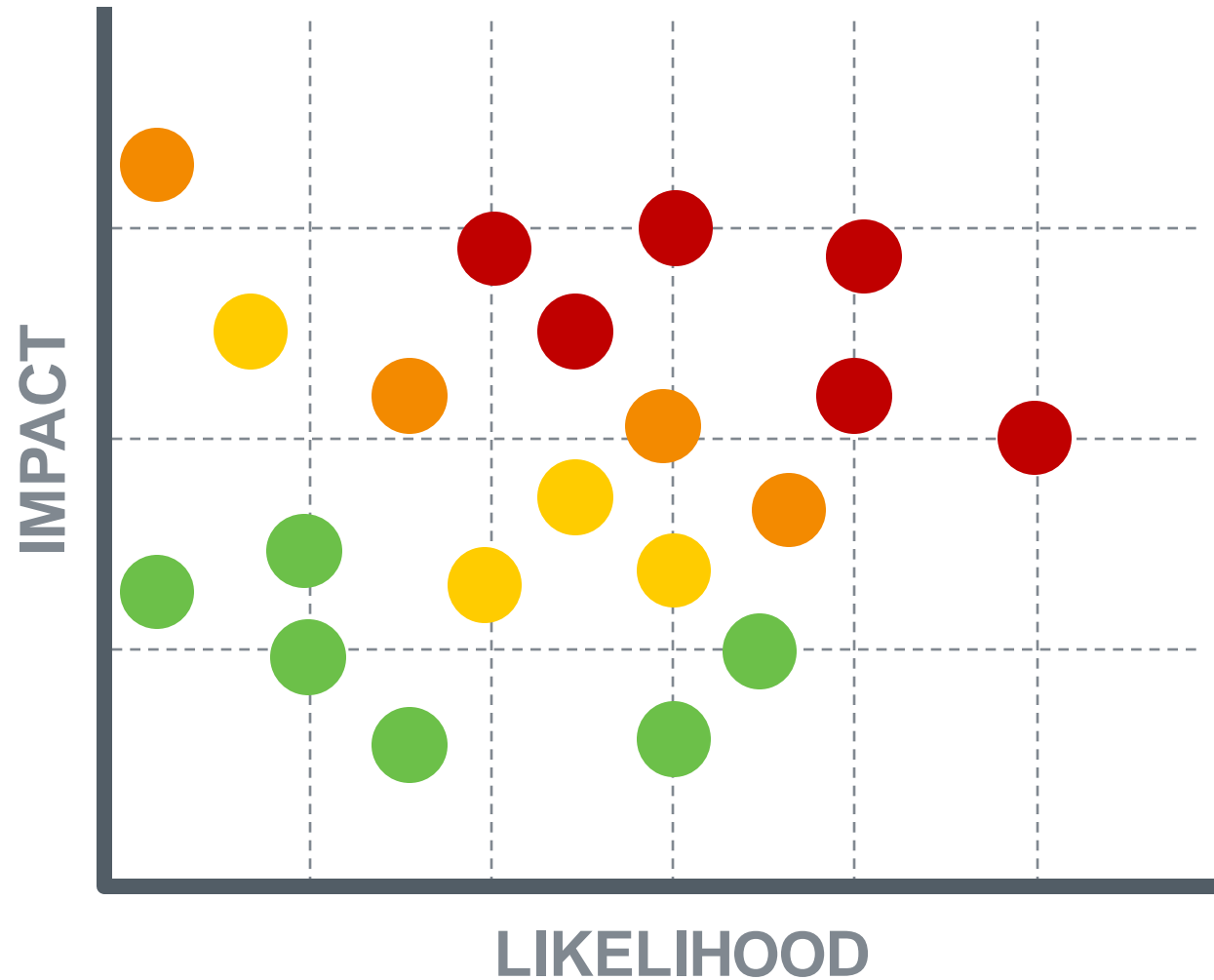


Intake Questions  
& Point Values

- |    |  |   |  |
|----|--|---|--|
| 12 | Service is essential to company operations         | 2 | Service is subject to regulatory requirements          |
| 6  | Annual contract amount > \$500,000                 | 2 | Third party has access to PII or PHI                   |
| 2  | A part of the service is performed internationally | 2 | Service is delivered as a cloud-based solution         |
| 2  | Difficult to replace service with alternative      | 2 | Third party has access to our technical infrastructure |
| 2  | High annual record volume                          | 2 | Third party outsources a portion of the service        |

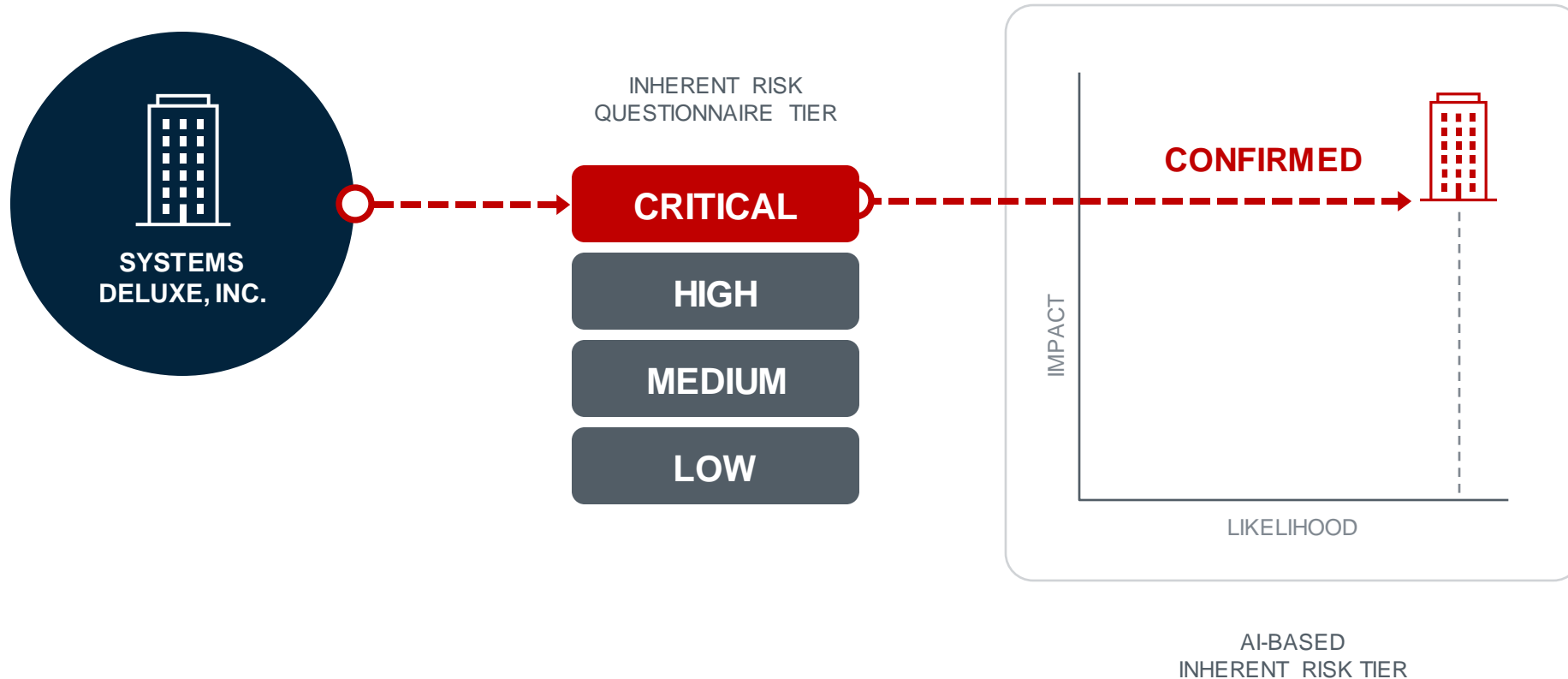
# Option 2: AI-Based Inherent Risk Calculation

MACHINE LEARNING ON LARGE DATA SETS CAN DETERMINE LIKELIHOOD AND IMPACT OF A BREACH



# Option 3: IRQ + AI

EMPLOY ARTIFICIAL INTELLIGENCE TO CONFIRM INHERENT RISK QUESTIONNAIRE RESPONSES





STEP TWO

# Scope & Schedule Your Assessments

# Inherent Risk Drives Scope & Review Schedule

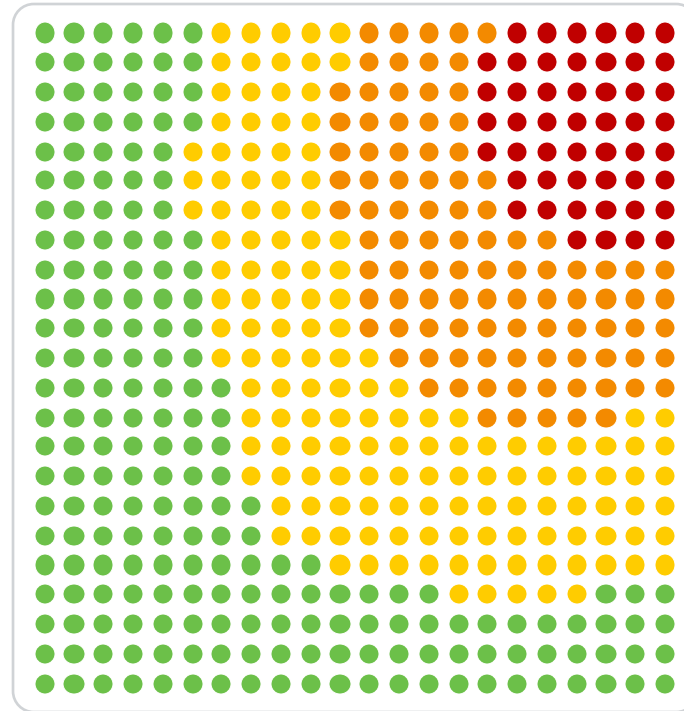
Inherent Risk		Previous Assessment Rating		Residual Risk	Assessment Scope	Assessment Frequency
CRITICAL	+	No Prior Review	=	Critical	Heavy	ASAP
		Unsatisfactory		Critical	Heavy	Annual
		Needs Improvement		Critical	Heavy	Annual
		Satisfactory		High	Medium	Annual
HIGH	+	No Prior Review	=	High	Medium	ASAP
		Unsatisfactory		High	Medium	Biennial
		Needs Improvement		High	Medium	Biennial
		Satisfactory		Medium	Light	Biennial
MEDIUM	+	No Prior Review	=	Medium	Light	ASAP
		Unsatisfactory		Medium	Light	Biennial
		Needs Improvement		Medium	Light	Biennial
		Satisfactory		Low	Light	Triennial
LOW	+	No Prior Review	=	Low	Predictive / AI	Predictive / AI
		Unsatisfactory		Low	Predictive / AI	Predictive / AI
		Needs Improvement		Low	Predictive / AI	Predictive / AI
		Satisfactory		Low	Predictive / AI	Predictive / AI

STEP THREE

# Import Completed Assessments via an Exchange

# Import Completed Assessments from an Exchange

COMPLETED, ATTESTED AND VALIDATED ASSESSMENTS SPEED DILIGENCE ACTIVITIES



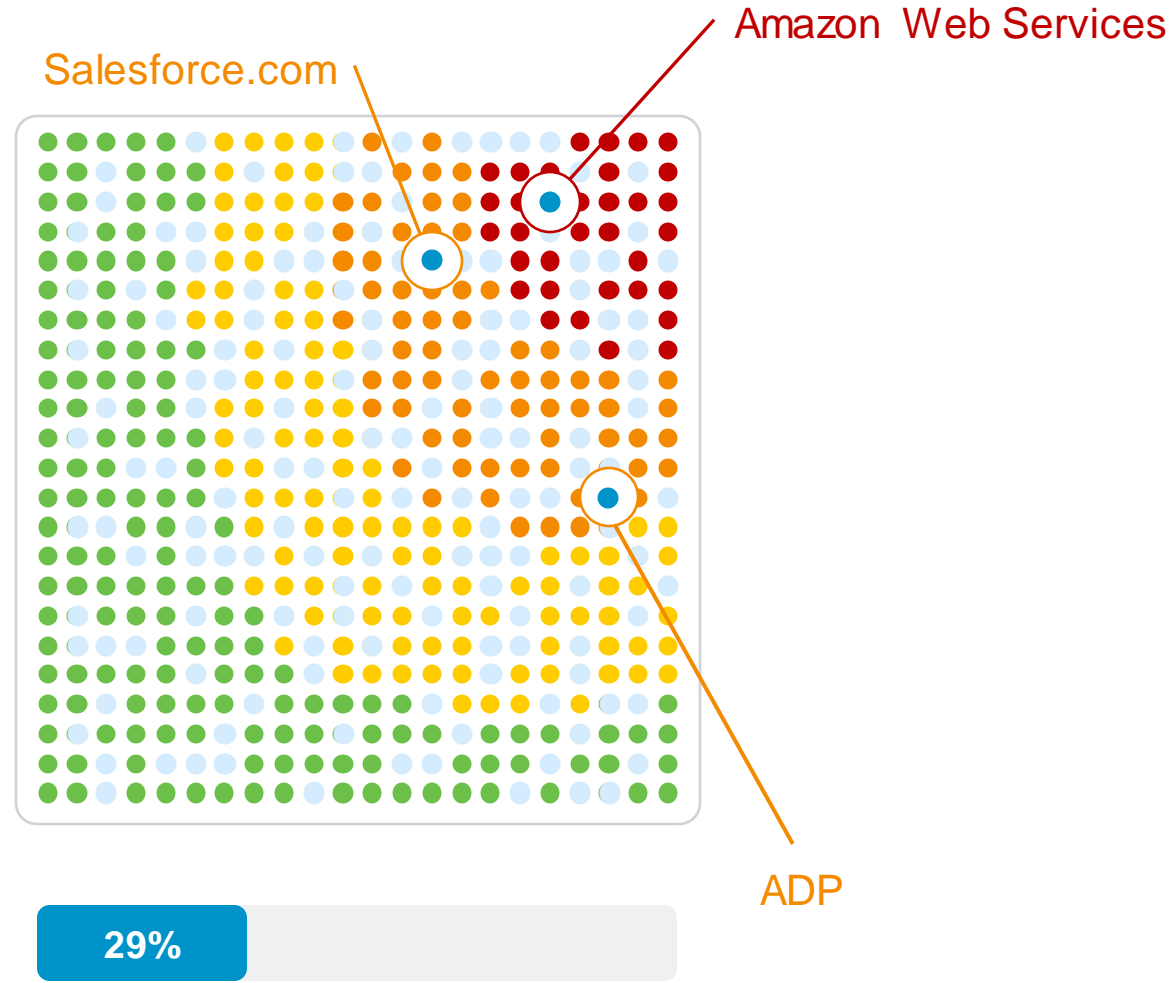


# Assess Large Third-Parties

COMPLETE ASSESSMENTS ON THE HARDEST-TO-ASSESS THIRD PARTIES

Large, hard-to-assess service providers prefer the exchange model to satisfy client due diligence demands.

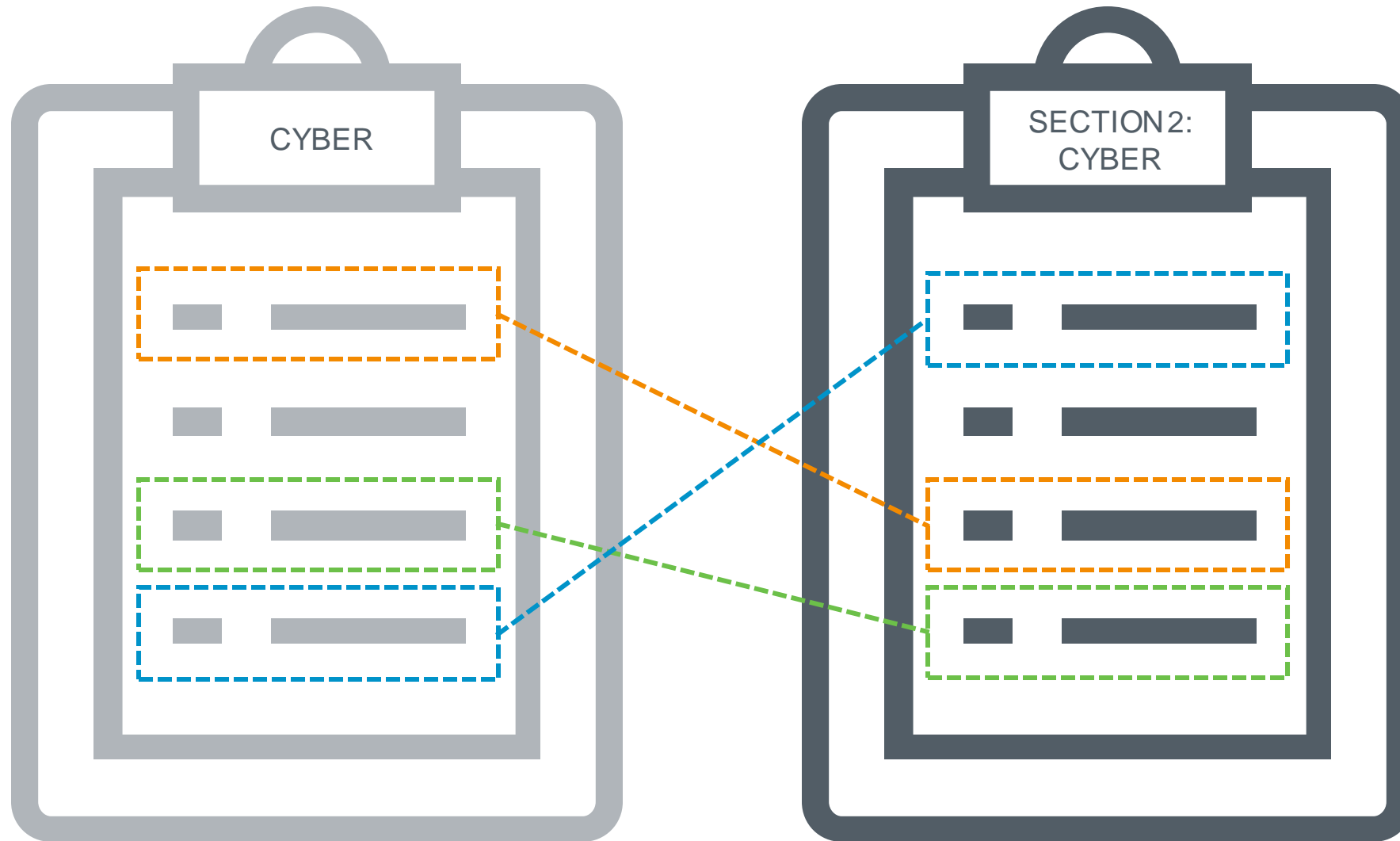
Exchanges give you access to assessment data you most likely couldn't get on your own.



STEP FOUR

# Augment Exchange Data with Supplemental Questions

# Map Your Questionnaire

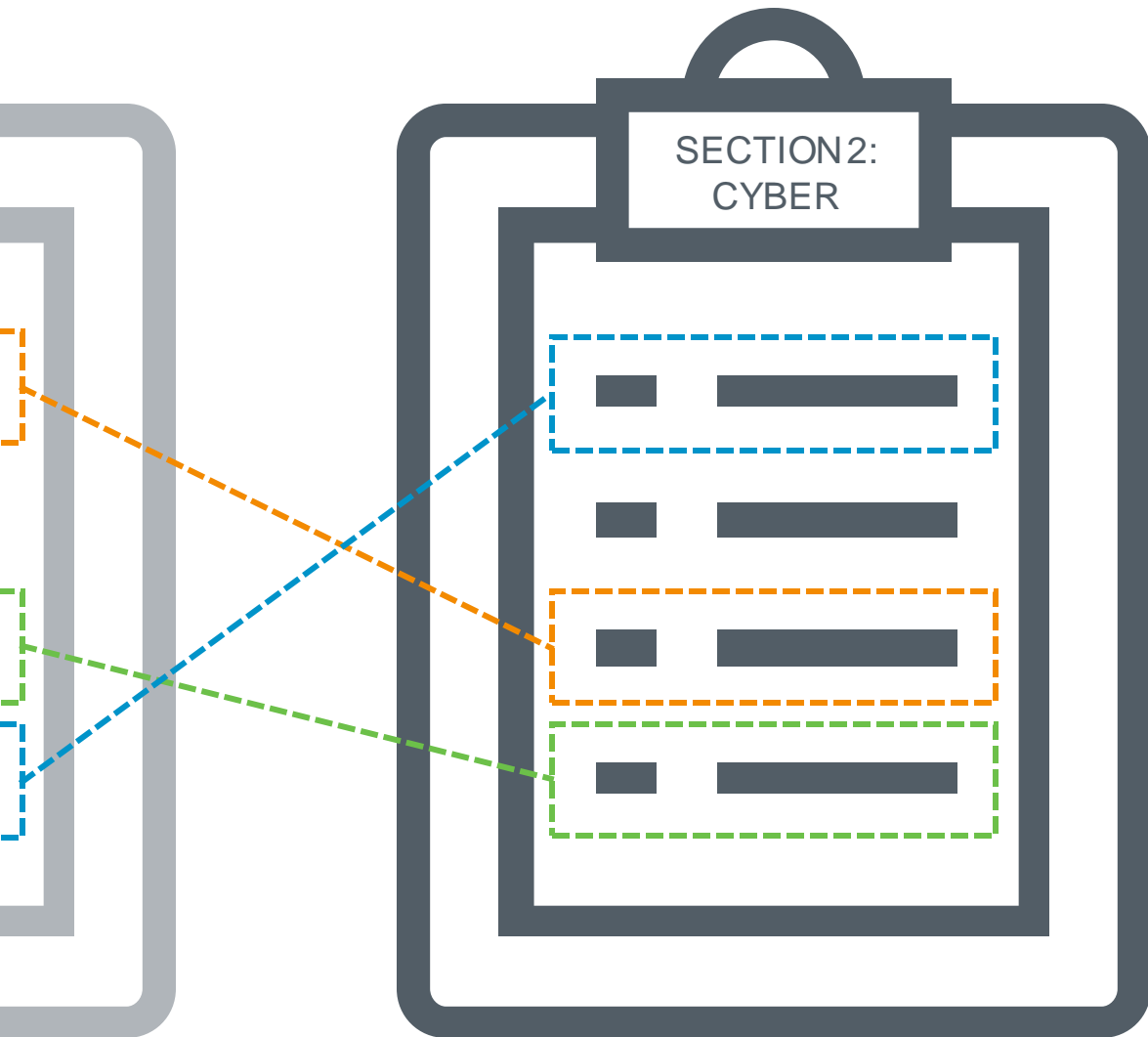


EXCHANGE QUESTIONNAIRE

YOUR QUESTIONNAIRE



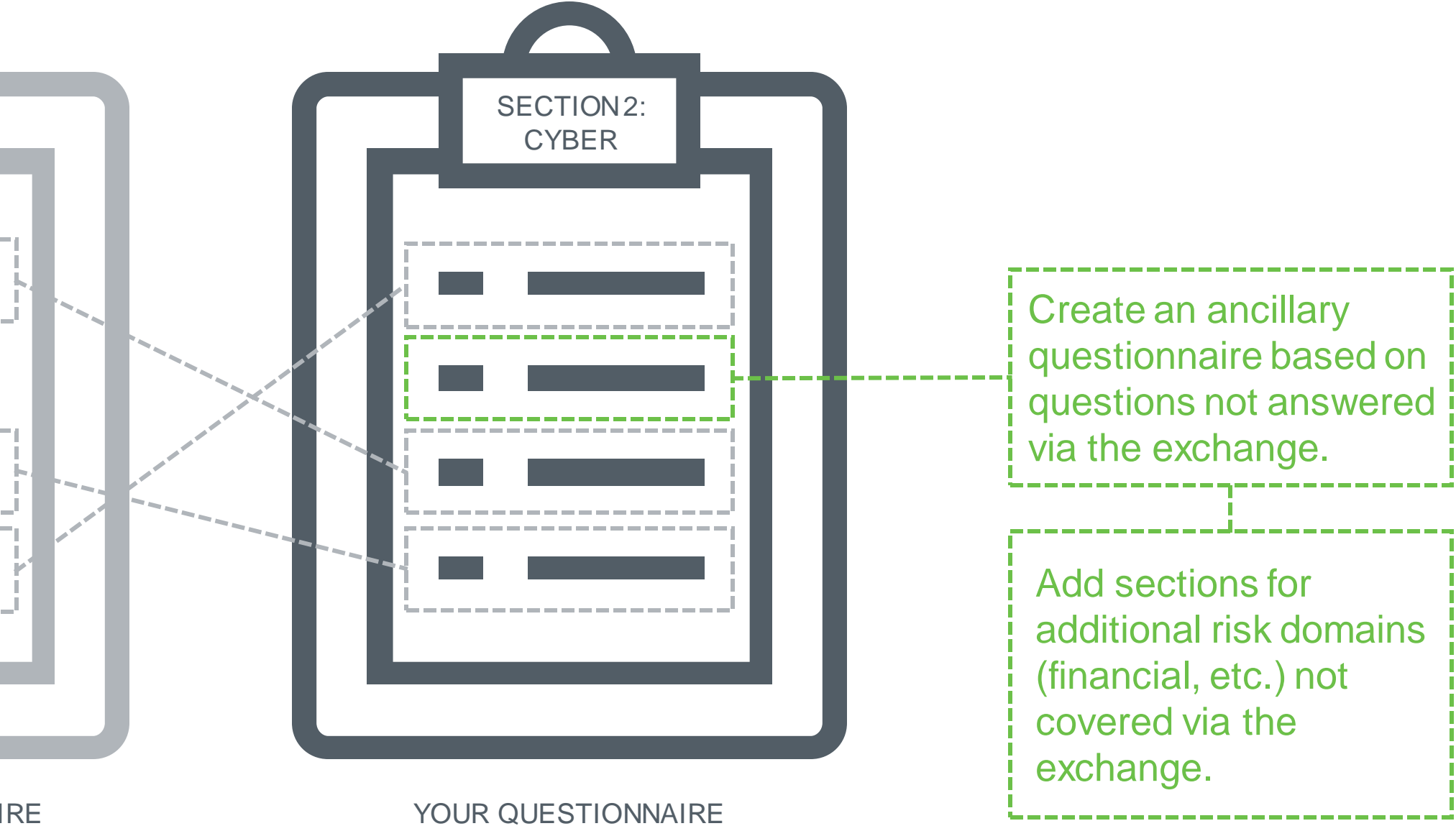
# Map Your Questionnaire



IRE

YOUR QUESTIONNAIRE

# Map Your Questionnaire

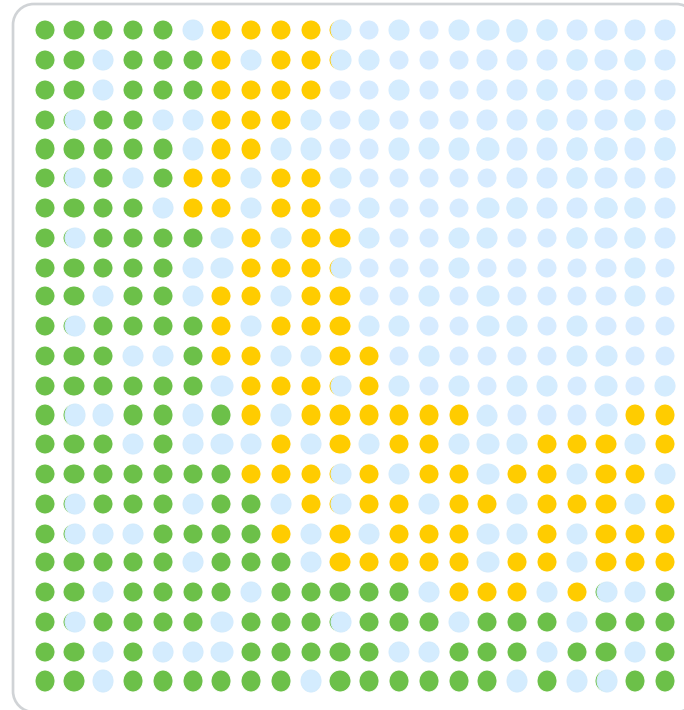


STEP FIVE

# Complete Assessments via Assessment Engine / Vendor Portal

# Complete High-Risk Assessment Work

Assess your remaining **Critical** and **High-Risk** third parties via your assessment engine



WORK COMPLETE

- Scoped by inherent risk
- Completed via vendor portal
- Documentation / attachments
- Question delegation
- Preferred responses / scoring

STEP SIX

# Confirm Responses with External Expert Data

# Expert Vendor Intelligence

- Cybersecurity Ratings:
  - BitSight
  - Black Kite
  - ProcessUnity (Global Risk Exchange)
  - RiskRecon
  - SecurityScorecard
- Financial Health Scores:
  - RapidRatings
  - Dun & Bradstreet
- Environmental, Social, Governance
  - EcoVadis
- ABAC / UBO / Adverse Media
  - LSEG (formerly Refinitiv)
  - Dun & Bradstreet
- Multiple Risk Domains
  - Interos
- Free Resources
  - Stock Tickers
  - Financial Filings
  - Google News Alerts

# Confirm Vendor Submissions

EXPERT VENDOR INTELLIGENCE

# Confirm Vendor Submissions

EXPERT VENDOR INTELLIGENCE

## Vendor Assessment Responses

YES	100%	YES	100%
GREAT	A+	GREAT	A+
YES	100%	YES	100%
GREAT	A+	GREAT	A+



# Confirm Vendor Submissions

EXPERT VENDOR INTELLIGENCE

## Vendor Assessment Responses

YES	100%	YES	100%
GREAT	A+	GREAT	A+
YES	100%	YES	100%
GREAT	A+	GREAT	A+

## Expert Vendor Intelligence

RapidRatings FHR: 72

# Confirm Vendor Submissions

EXPERT VENDOR INTELLIGENCE

## Vendor Assessment Responses

YES	100%	YES	100%
GREAT	A+	GREAT	A+
YES	100%	YES	100%
GREAT	A+	GREAT	A+

## Expert Vendor Intelligence

RapidRatings FHR: 72

BitSight Security Rating: 680

# Confirm Vendor Submissions

## EXPERT VENDOR INTELLIGENCE

### Vendor Assessment Responses

YES	100%	YES	100%
GREAT	A+	GREAT	A+
YES	100%	YES	100%
GREAT	A+	GREAT	A+

### Expert Vendor Intelligence

RapidRatings FHR: 72

BitSight Security Rating: 680

World-Check One Positive Results: 2

# Confirm Vendor Submissions

## EXPERT VENDOR INTELLIGENCE

### Vendor Assessment Responses

YES	100%	YES	100%
GREAT	A+	GREAT	A+
YES	100%	YES	100%
GREAT	A+	GREAT	A+

### Expert Vendor Intelligence

RapidRatings FHR: 72

BitSight Security Rating: 680

World-Check One Positive Results: 2

EcoVadis Ethics Score: 30

STEP SEVEN

# Accelerate Policy Reviews

# The Four Policy Review Personas

## SKIPPERS

Do not review policy documentation during due diligence.

**FASTEST!**  
**CHEAPEST!**  
**RISKIEST!**

## SKIMMERS

Skim policy documentation for key points.

**FAST!**  
**CHEAP!**  
**RISKY!**

## READERS

Spend the time to completely review all policy documentation.

**SLOW!**  
**LABORIOUS!**  
**LESS RISK!**

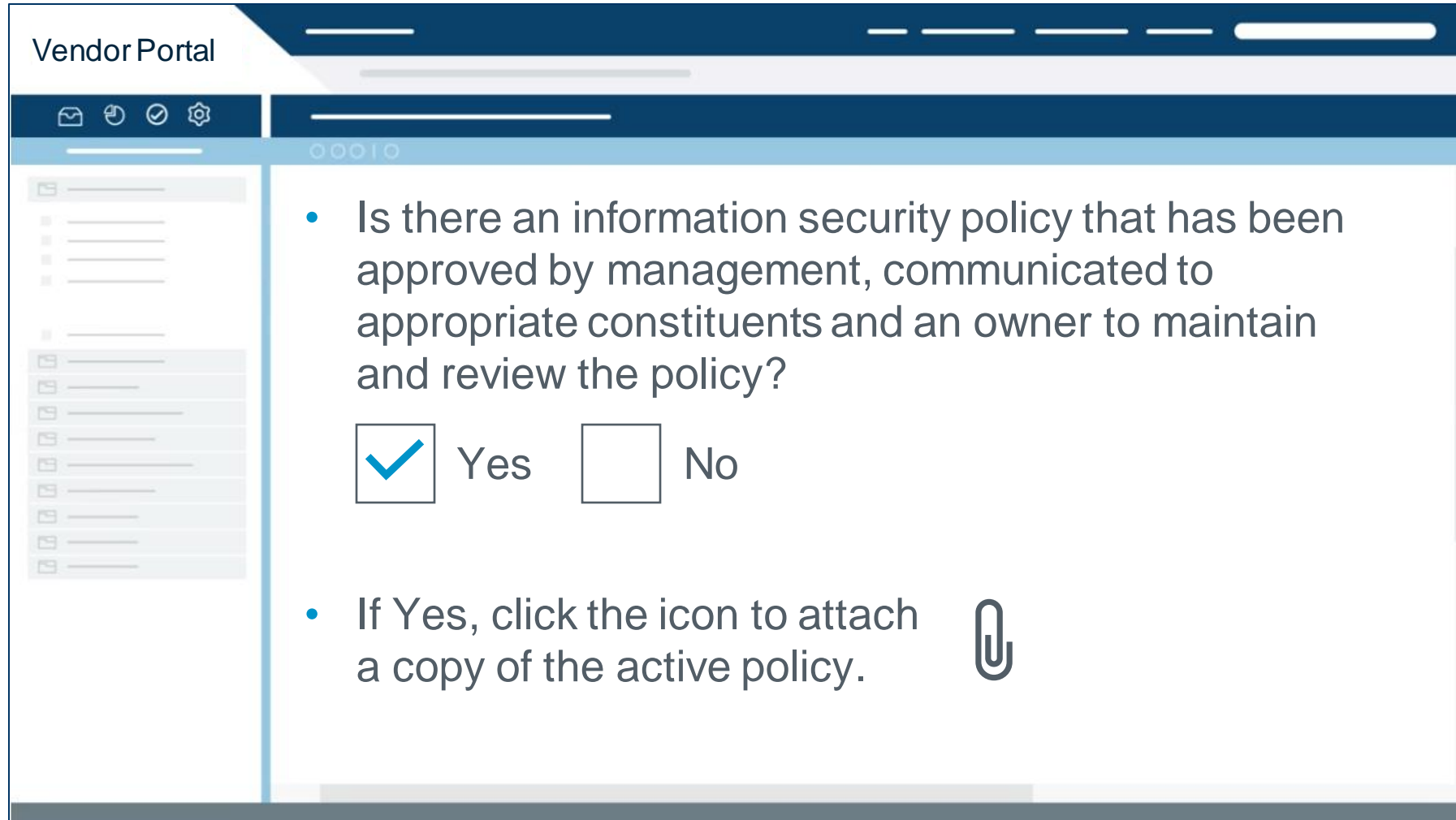
## OUTSOURCERS

Pay someone to review all policy documentation.

**COSTLY!**  
**LESS RISK!**

# Extend Your Team with Artificial Intelligence

SIGNIFICANTLY REDUCE TIME TO COMPLETE DUE DILIGENCE




The screenshot shows a web application interface for a 'Vendor Portal'. The top navigation bar is dark blue with the text 'Vendor Portal' on the left and several white horizontal lines on the right. Below the navigation bar is a dark blue sidebar containing icons for mail, refresh, checkmark, and settings. The main content area is white and contains a list of items on the left and a large text area on the right. The text area contains a question and two radio button options.

Vendor Portal

Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?

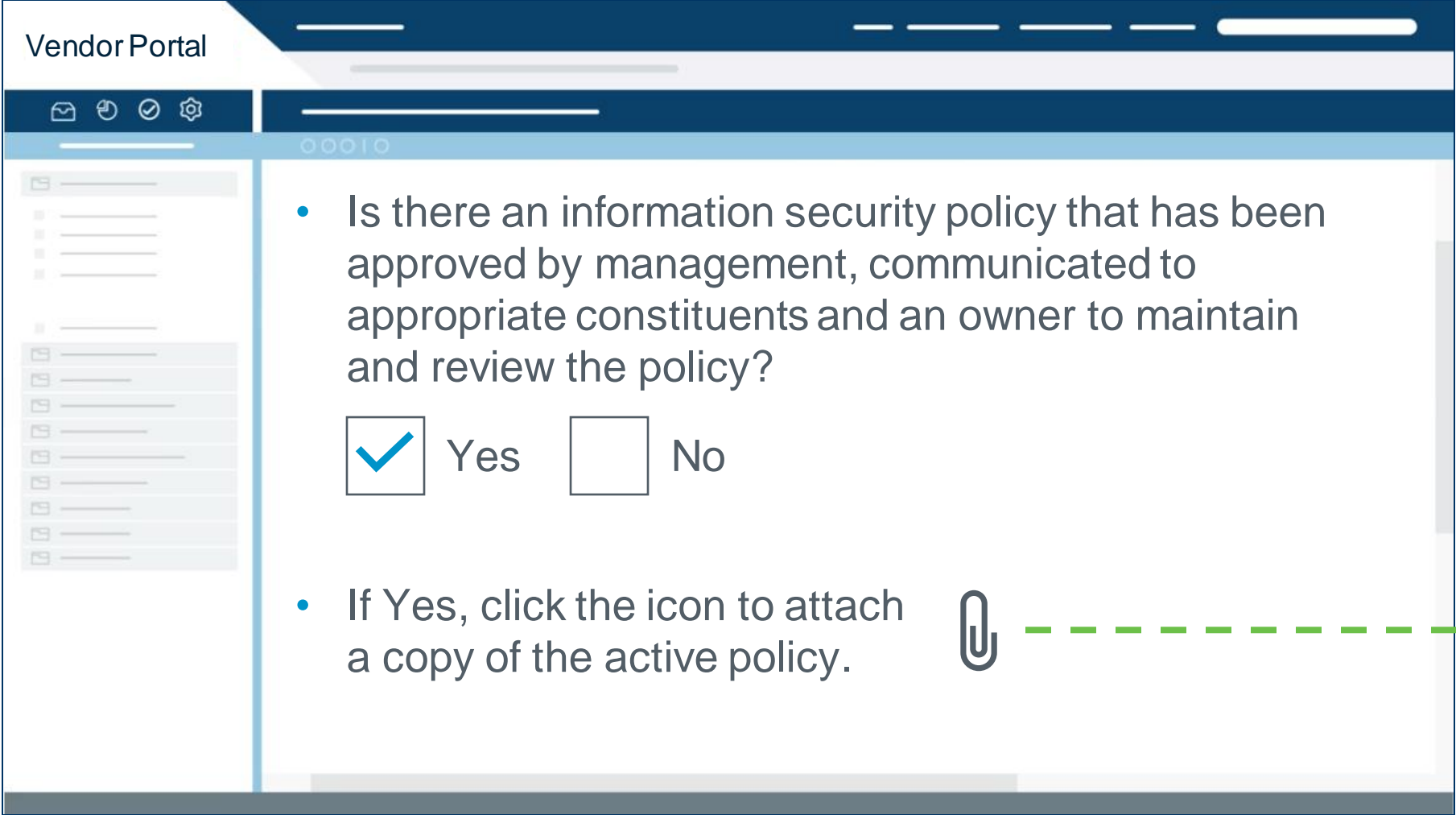
Yes  No

If Yes, click the icon to attach a copy of the active policy.



# Extend Your Team with Artificial Intelligence

SIGNIFICANTLY REDUCE TIME TO COMPLETE DUE DILIGENCE



Vendor Portal

- Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?  
 Yes  No
- If Yes, click the icon to attach a copy of the active policy.

The screenshot shows a web interface for a 'Vendor Portal'. It features a dark blue header with the text 'Vendor Portal' and a navigation bar with icons for mail, refresh, check, and settings. Below the navigation bar is a sidebar with a list of items, each with a folder icon. The main content area displays a questionnaire item with a blue checkmark in a box next to the 'Yes' option. A paperclip icon is positioned to the right of the second question, with a dashed green line extending from it towards the right side of the slide.



AI-Powered Policy Analysis

The icon features a white silhouette of a human head in profile, facing right. Inside the head, there is a stylized circuit board or neural network pattern in white. Below the head, the text 'AI-Powered Policy Analysis' is written in white, sans-serif font. A dashed green arrow points upwards from the bottom of the icon area towards the right side of the slide.



# Extend Your Team with Artificial Intelligence

SIGNIFICANTLY REDUCE TIME TO COMPLETE DUE DILIGENCE

Vendor Assessment

- Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?
- File: [baldwin\\_2023\\_infosec\\_v3.3.pdf](#)
- Rating: **Good**

**85** / 100

AI-Powered  
Policy Analysis

# Extend Your Team with Artificial Intelligence

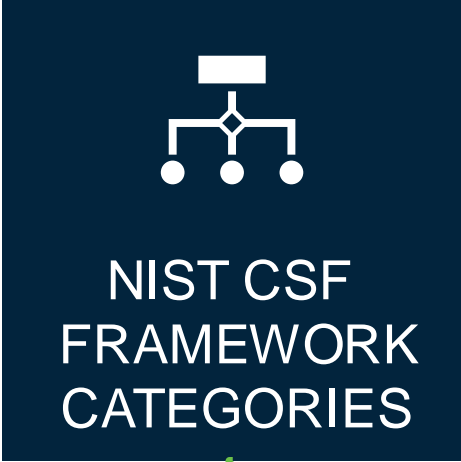
SIGNIFICANTLY REDUCE TIME TO COMPLETE DUE DILIGENCE

Vendor Assessment

- File: baldwin\_2023\_infosec\_v3.3.pdf
- Rating: **Good**

**85 / 100**

ID.AM	ID.RM	PR.AT	PR.DS	PR.IP	PR.PT
90	30	50	30	15	85

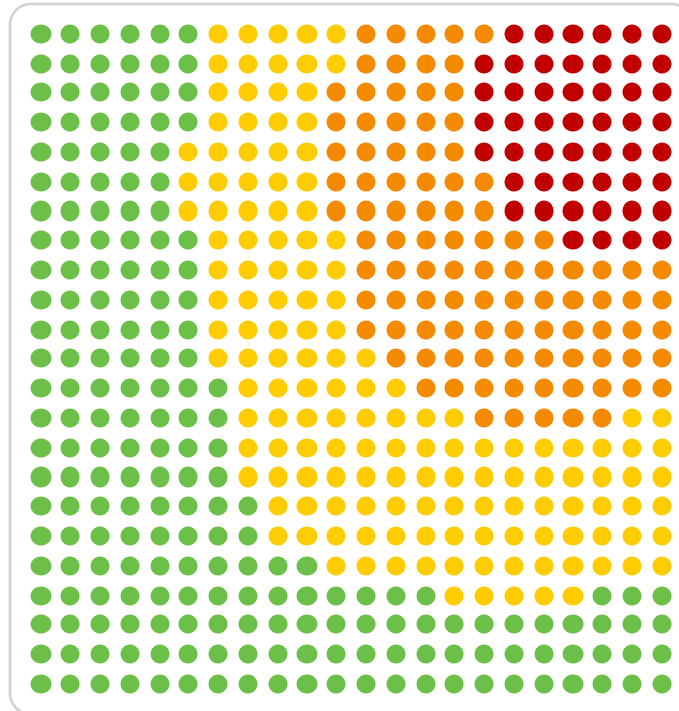


STEP EIGHT

# Employ AI to Assess / Monitor Lower-Risk Third Parties

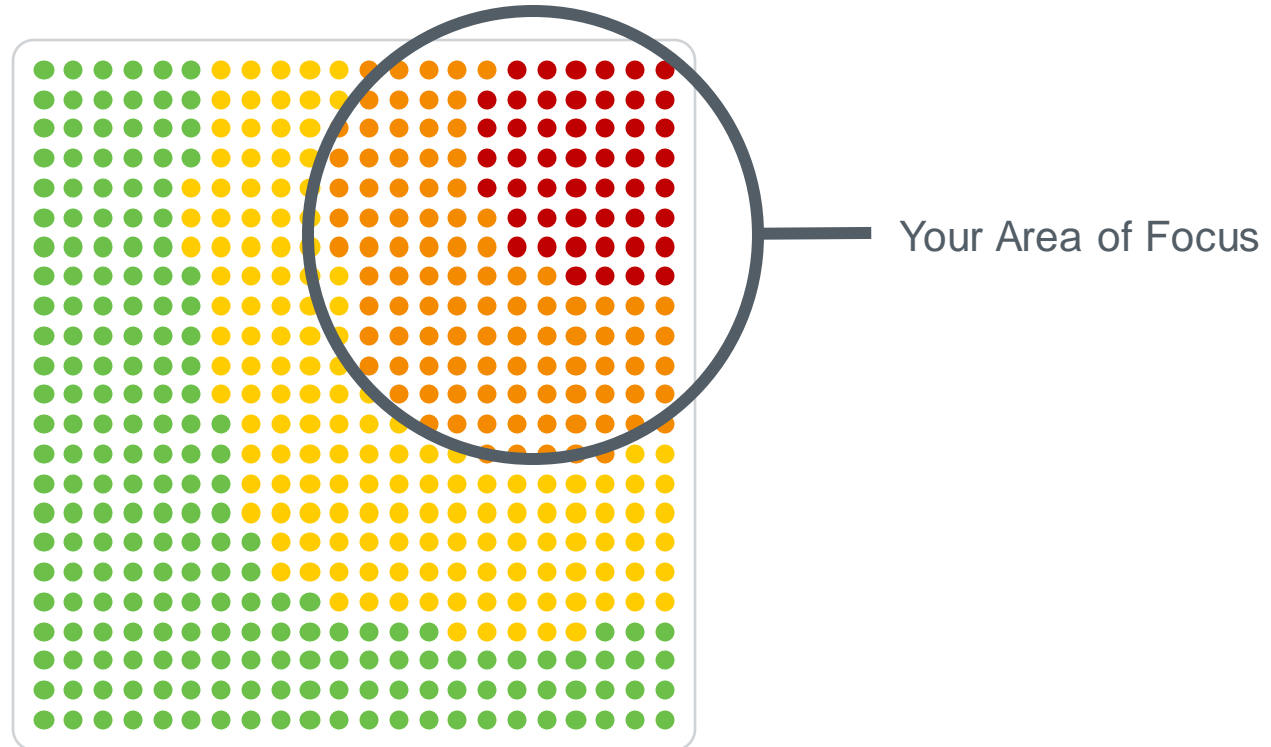
# Extend Your Team with Artificial Intelligence

ASSESS LOWER RISK THIRD PARTIES YOU DON'T HAVE TIME TO ASSESS



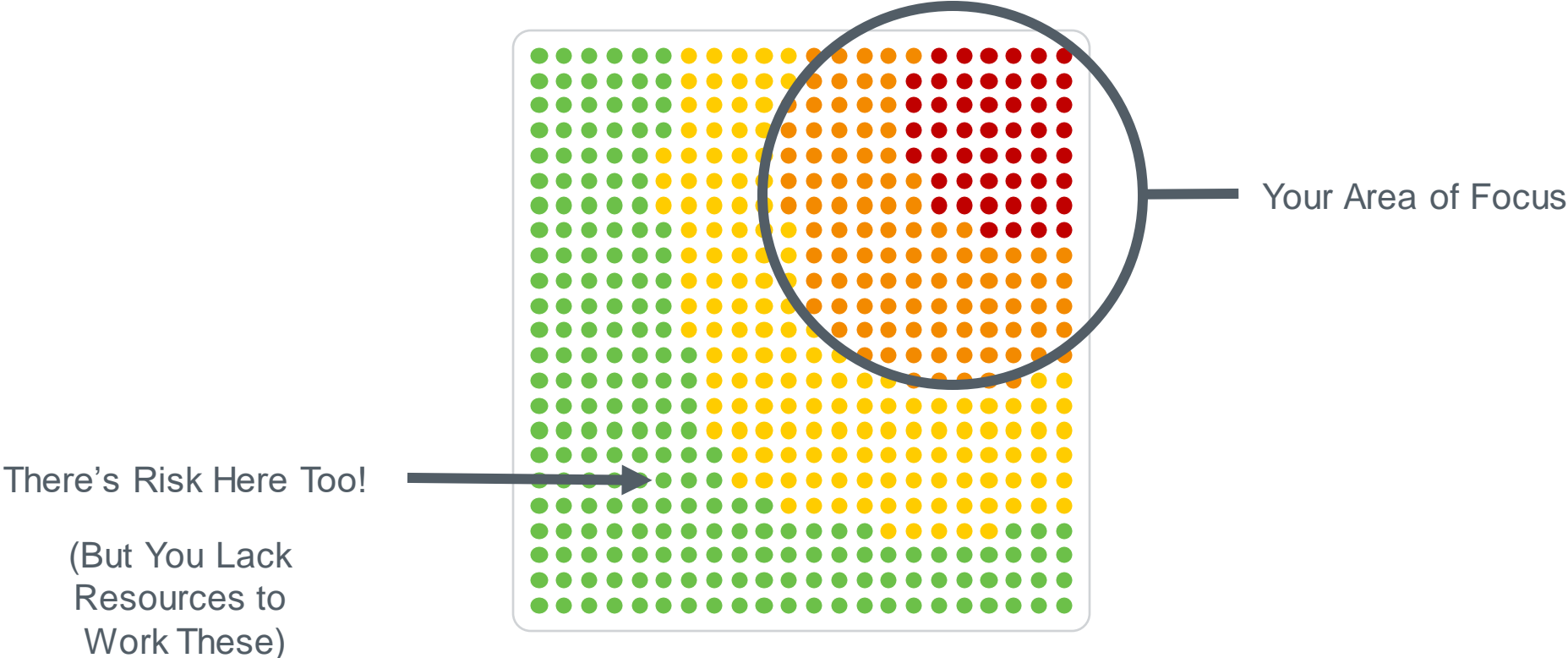
# Extend Your Team with Artificial Intelligence

ASSESS LOWER RISK THIRD PARTIES YOU DON'T HAVE TIME TO ASSESS



# Extend Your Team with Artificial Intelligence

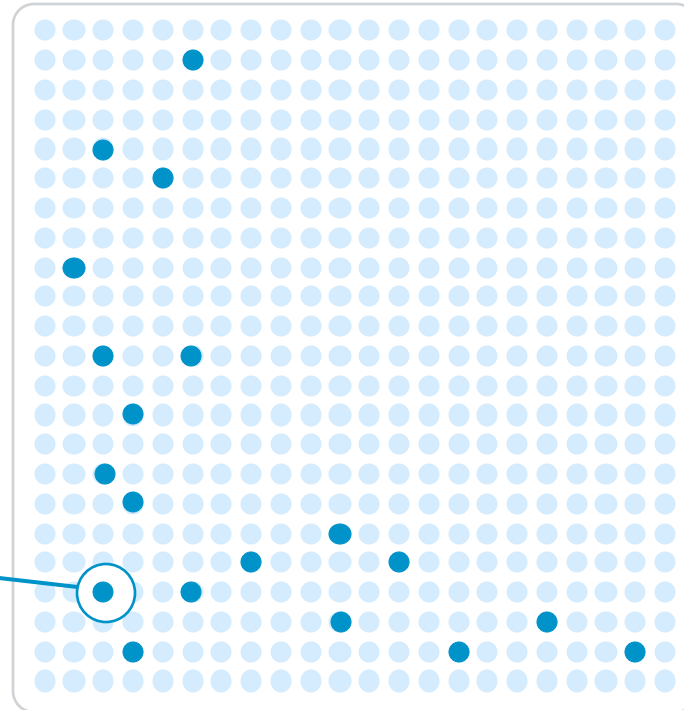
ASSESS LOWER RISK THIRD PARTIES YOU DON'T HAVE TIME TO ASSESS



# Extend Your Team with Artificial Intelligence

AUGMENT YOUR TEAM TO EXTEND COVERAGE TO YOUR ENTIRE ECOSYSTEM

**Low Confidence Score:**  
Requires Additional Analysis



- AI anticipates how a third-party will answer assessment questions with high fidelity
- Under-performing third-parties are identified for additional analysis and assessment work



WORK COMPLETE

STEP NINE

# Set Up Continuous Monitoring



# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE

# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE

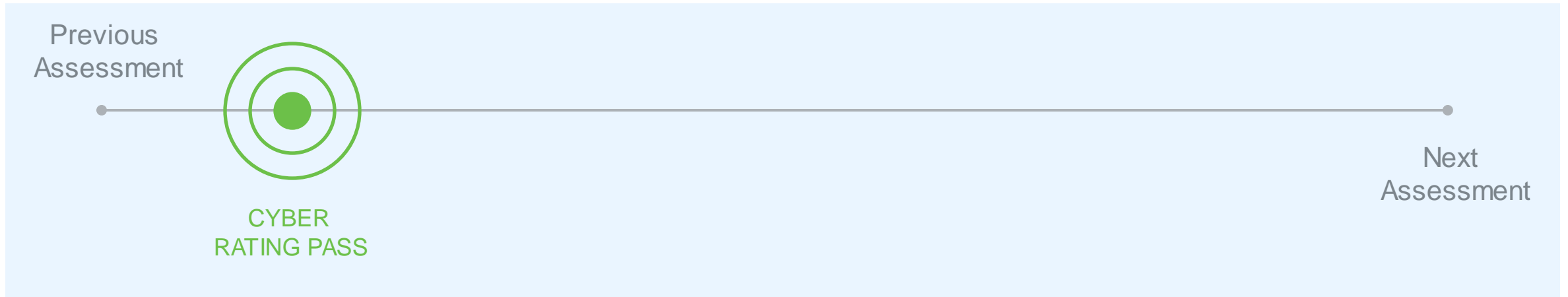
Previous  
Assessment



Next  
Assessment

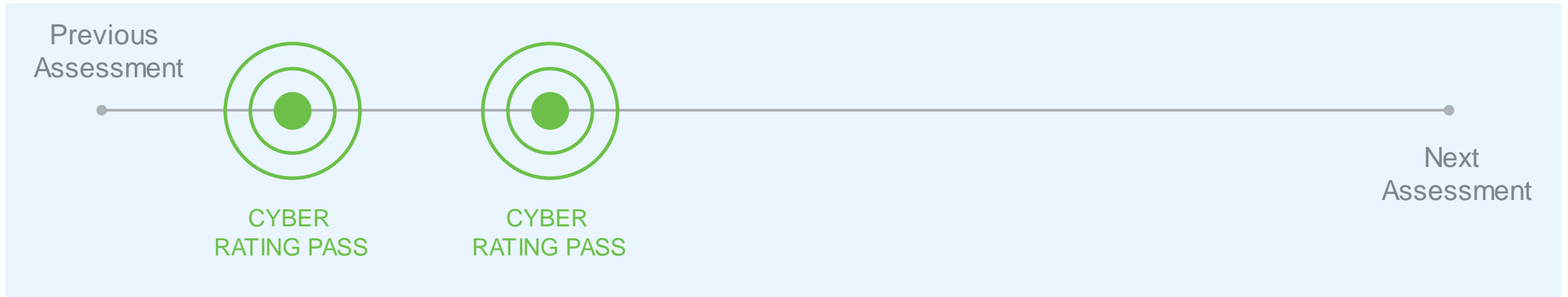
# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



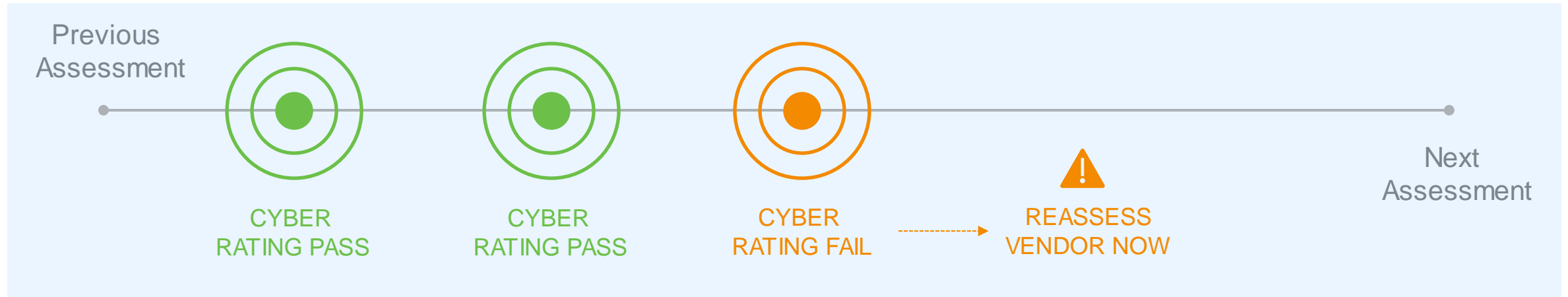
# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



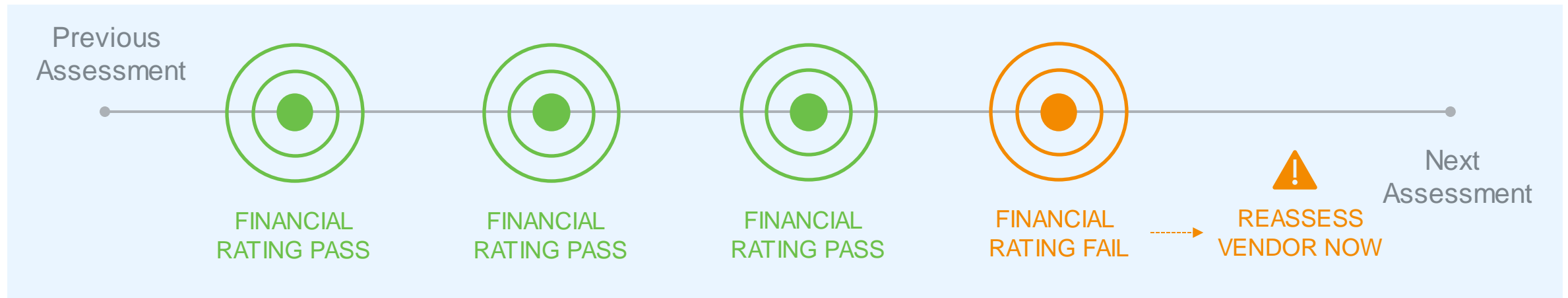
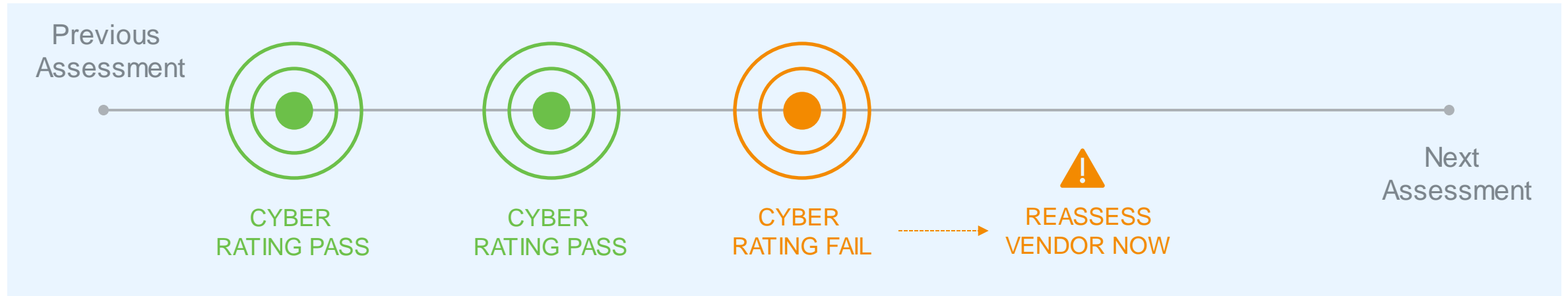
# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



# Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



STEP TEN

# Measure & Report



# Tracking Program Performance

- Average Time to Onboard
- Assessment Completion Rate
- Assessment Backlog
- Due Diligence Completion Time
- Portfolio Assessment Coverage
- Risk Remediation Time
- Service Satisfaction Rate
- Third-Party Compliance Rate
- Third-Party Cost Savings
- Third-Party Incident Rate
- Third-Party Spend
- Vendor Concentration
- Vendor Diversity
- Overall Program Costs



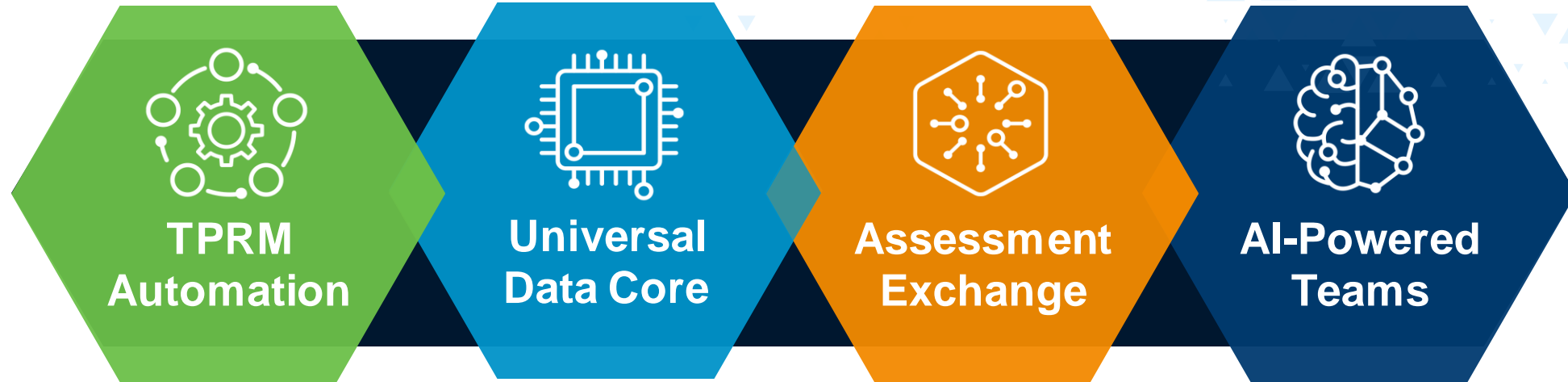
# Vendor Assessments Reimagined

MODERN, MATURE THIRD-PARTY RISK MANAGEMENT

1.	Classify Vendors via Inherent Risk	 
2.	Scope & Schedule Assessments	
3.	Import Completed Assessments from an Exchange	 
4.	Augment Exchange Data with Supplemental Questions	
5.	Complete Assessments via Assessment Engine / Vendor Portal	

6.	Confirm Responses with External Expert Data	 
7.	Accelerate Vendor Policy Reviews	
8.	Monitor Lower-Risk Third Parties	 
9.	Set Up Continuous Monitoring	 
10.	Measure & Report	 

# TPRM Foundational Components



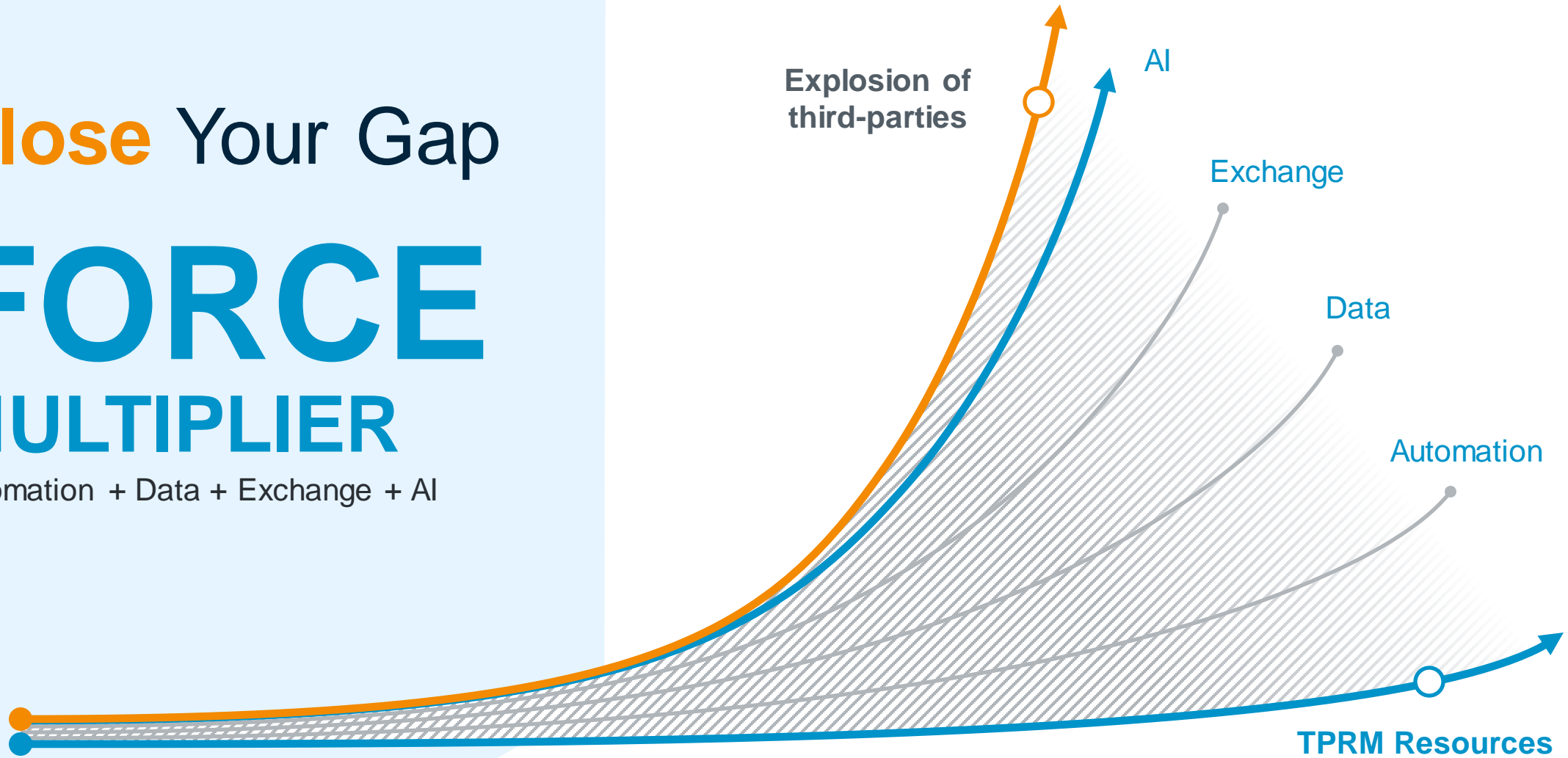
The Force Multiplier Comes from the Four  
Critical Components for Modern TPRM

THE DISRUPTIVE OPPORTUNITY

Close Your Gap

# FORCE MULTIPLIER

Automation + Data + Exchange + AI



# Modern, Mature Third-Party Risk Management

## Integrity

Maximize confidence

## People

Elevate human performance



**FORCE  
MULTIPLIER**

Across Your TPRM Program

## Coverage

Scale from tens to hundreds to thousands

## Speed

Accelerate diligence & actions

# High Efficiency Assessments



Prioritize  
assessment work  
based on inherent  
risk



Assess traditionally  
“hard to assess” third  
parties



Reduce the number  
of assessments you  
perform overall



Keep tabs on medium-  
and low-risk vendors  
without additional  
resources



Extend coverage to  
more third parties  
and catch up on  
assessment backlog

# Helping You Make the Shift to a Modern TPRM Program

FROM  
**Managing Assessments**

TO  
**Mitigating Risk**

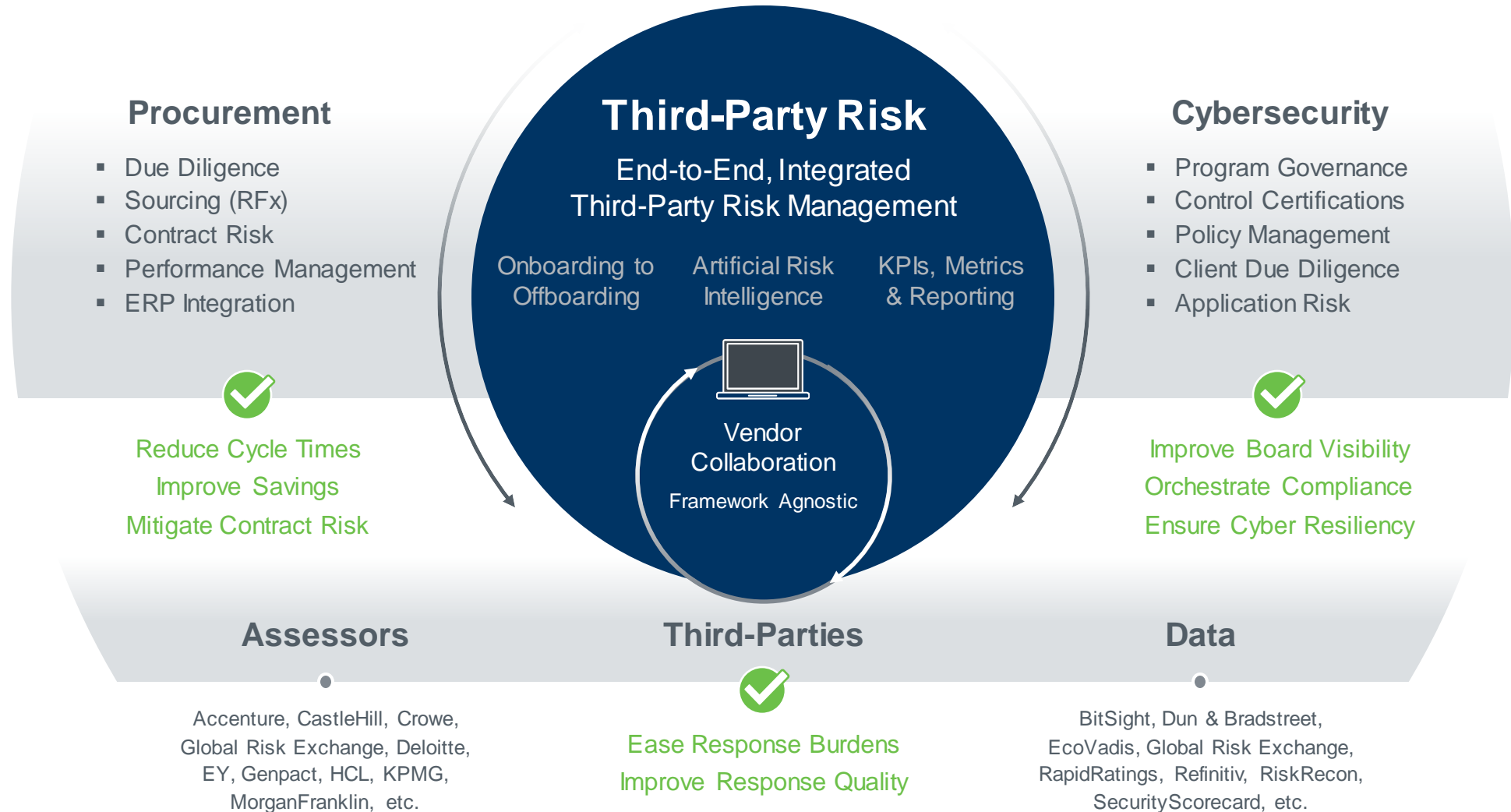


Compliance checklist	PURPOSE	Risk steward / growth enabler
Periodic	CADENCE	Continuous
Top tier	COVERAGE	Every third-party
Hundreds	VOLUME	Tens of thousands
Under-appreciated task	TPRM ROLE	Career-builder



# The Vision

## THE ENTERPRISE THIRD-PARTY + CYBERSECURITY ECOSYSTEM



# For More Information

**Automate Your Third-Party  
Risk Management Program:**

[www.processunity.com/third-party-risk-management/](http://www.processunity.com/third-party-risk-management/)

**Contact ProcessUnity:**

[www.processunity.com/contact](http://www.processunity.com/contact)

**Contact Ed Thomas:**

[ed.thomas@processunity.com](mailto:ed.thomas@processunity.com)

