

Best Practices: Post-Contract Vendor Monitoring

THIRD-PARTY RISK MANAGEMENT



ProcessUnity 

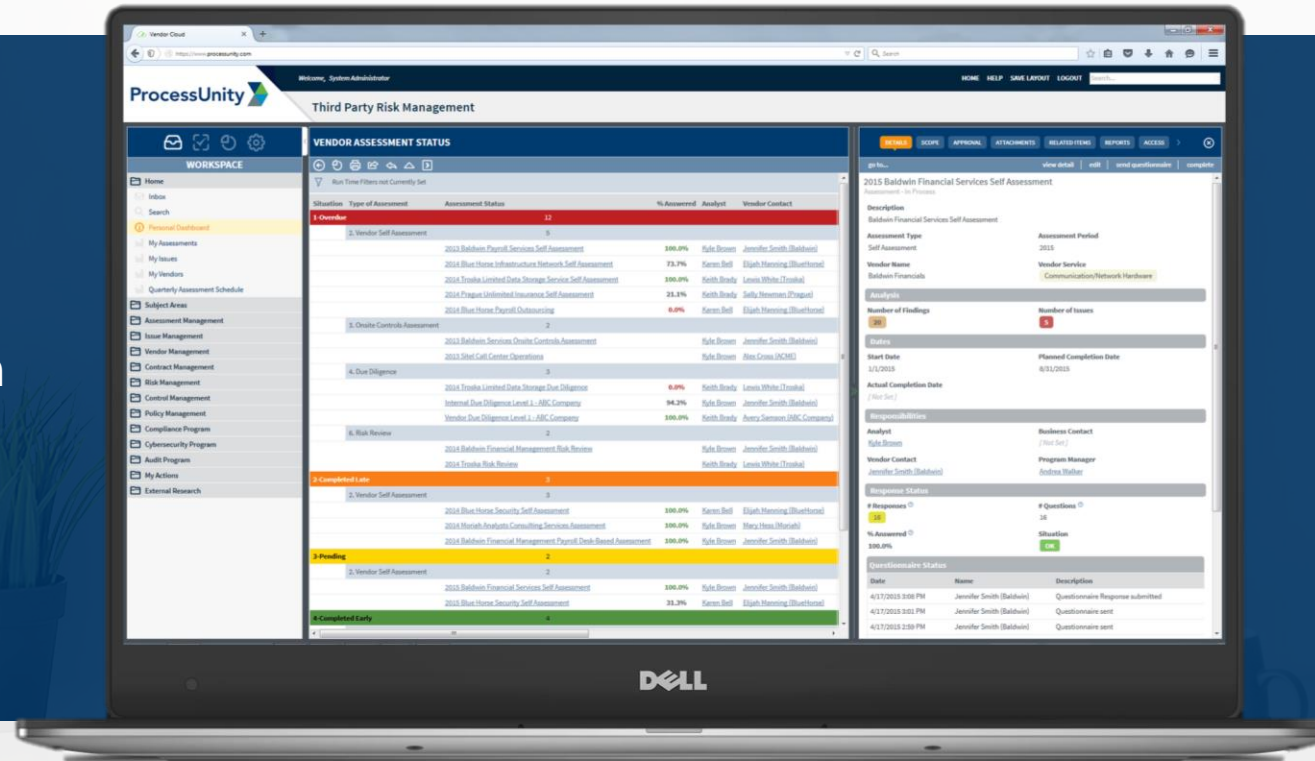
Today's Presenter



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

- Why Ongoing Vendor Monitoring?
- The Ongoing Monitoring Process
- Building the Schedule
- Unexpected Risks
- Expert Vendor Intelligence
- Next-Level Strategies
- Review & Next Steps
- Questions & Discussion



THIRD-PARTY RISK MANAGEMENT

What is Ongoing Vendor Monitoring?

The Third-Party Risk Lifecycle



Onboarding

Establish an enterprise-wide process



Due Diligence

Enforce objectivity within your vendor process



Ongoing Monitoring

Streamline processes while reducing errors



On-Site Control Assessment

Systematically conduct and document



Performance Reviews

Manage with consistency



Contract Reviews

Create a unified process



SLA Monitoring

Document, monitor and record



Issue Management

Formally track vendor issues

Signing a contract with a vendor isn't the end...It's the beginning.

START

Risk Can (and Will) Change Over Time

Risk Can (and Will) Change Over Time

Your organization's
risk appetite will
change over time.

Risk Can (and Will) Change Over Time

Your organization's risk appetite will change over time.

Your vendors' risk profiles will change over time.

Risk Can (and Will) Change Over Time

Your organization's risk appetite will change over time.

Your vendors' risk profiles will change over time.

It's critical to monitor these changes over time to reduce unnecessary risks.

Focus on Ongoing Monitoring



Onboarding

Establish an enterprise-wide process



Due Diligence

Enforce objectivity within your vendor process



Ongoing Monitoring

Streamline processes while reducing errors



On-Site Control Assessment

Systematically conduct and document



Performance Reviews

Manage with consistency



Contract Reviews

Create a unified process



SLA Monitoring

Document, monitor and record




Issue Management

Formally track vendor issues

The Goal: Ongoing Vendor Monitoring



The Process: Ongoing Vendor Monitoring



Conduct periodic “check-in” assessments related to your vendors’ controls to surface risks so you can take action.

Who Owns Ongoing Monitoring?

Who Owns Ongoing Monitoring?



PROCUREMENT

Responsible for
Onboarding New
Third Parties

Who Owns Ongoing Monitoring?



PROCUREMENT

Responsible for
Onboarding New
Third Parties

VS



INFORMATION SECURITY

Responsible for Data
Privacy / Protection and
Information Security Protection

Who Owns Ongoing Monitoring?



PROCUREMENT

Responsible for
Onboarding New
Third Parties



INFORMATION SECURITY

Responsible for Data
Privacy / Protection and
Information Security Protection

POLL QUESTION:

- Which team owns ongoing vendor monitoring in your organization?
 1. Procurement
 2. Information Security
 3. Procurement & Information Security (Shared)
 4. Other / Don't Know

Who Owns Ongoing Monitoring?



PROCUREMENT

Responsible for
Onboarding New
Third Parties



INFORMATION SECURITY

Responsible for Data
Privacy / Protection and
Information Security Protection

Who Does the Work?



PROCUREMENT

Responsible for
Onboarding New
Third Parties



INFORMATION SECURITY

Responsible for Data
Privacy / Protection and
Information Security Protection



SUBJECT MATTER EXPERTS

Experts from Lines-of-Business

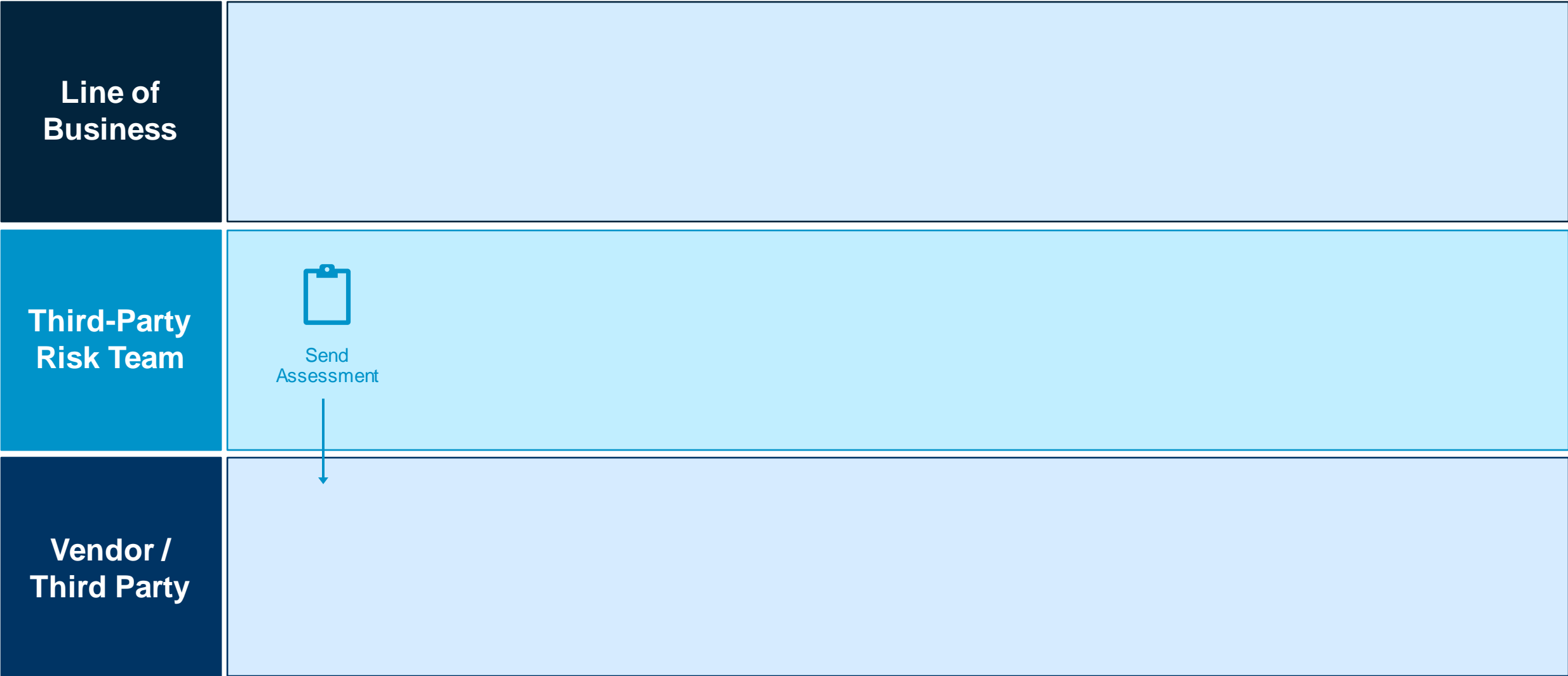
THIRD-PARTY RISK MANAGEMENT

Getting Started: The Ongoing Vendor Monitoring Process

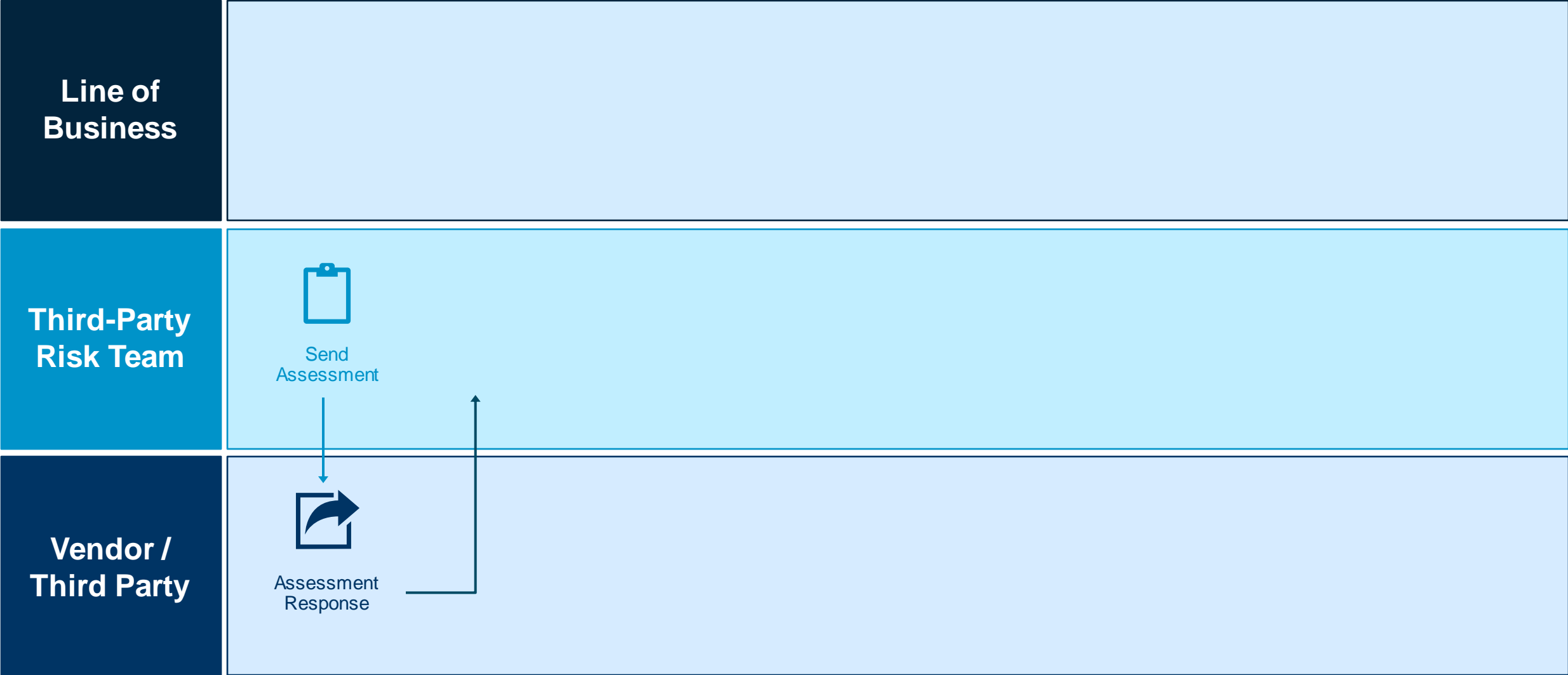
Ongoing Monitoring: Periodic Due Diligence

Line of Business	
Third-Party Risk Team	
Vendor / Third Party	

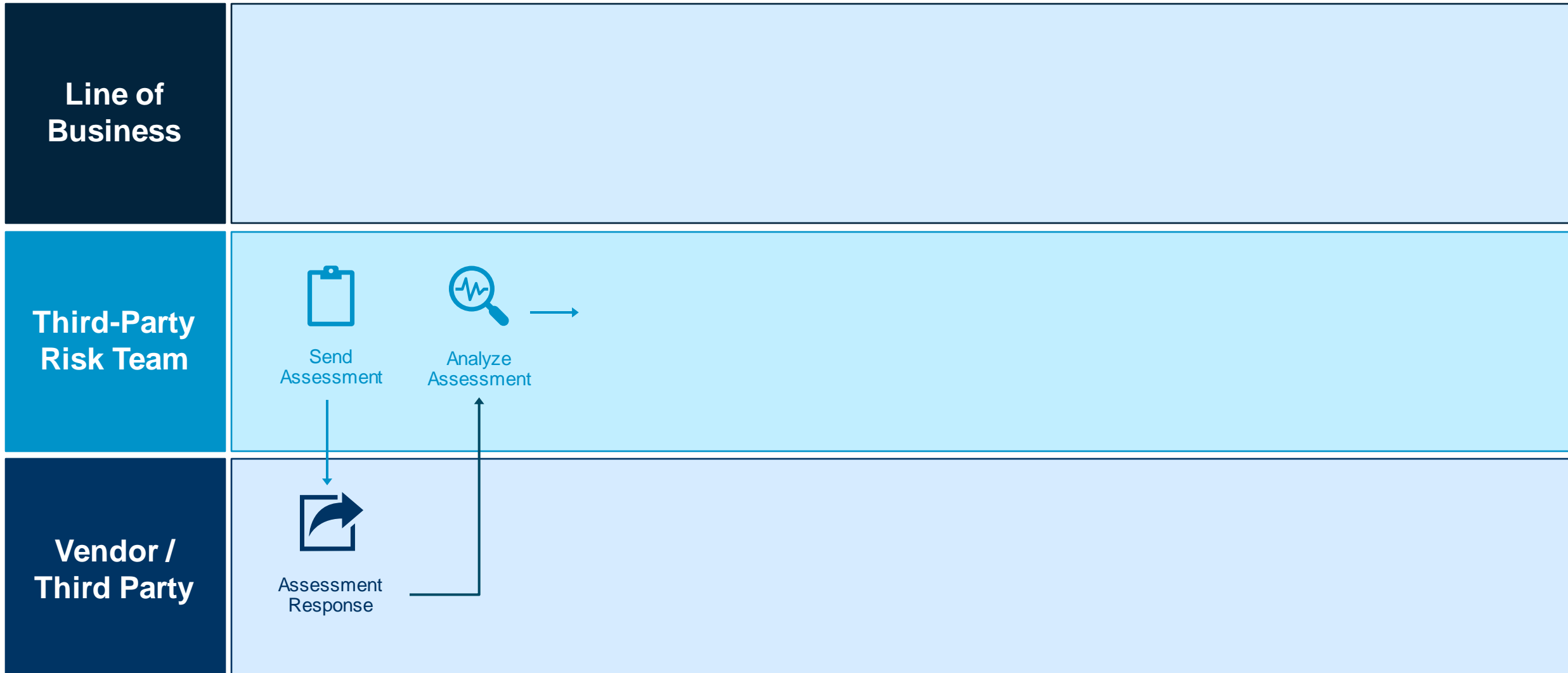
Ongoing Monitoring: Periodic Due Diligence



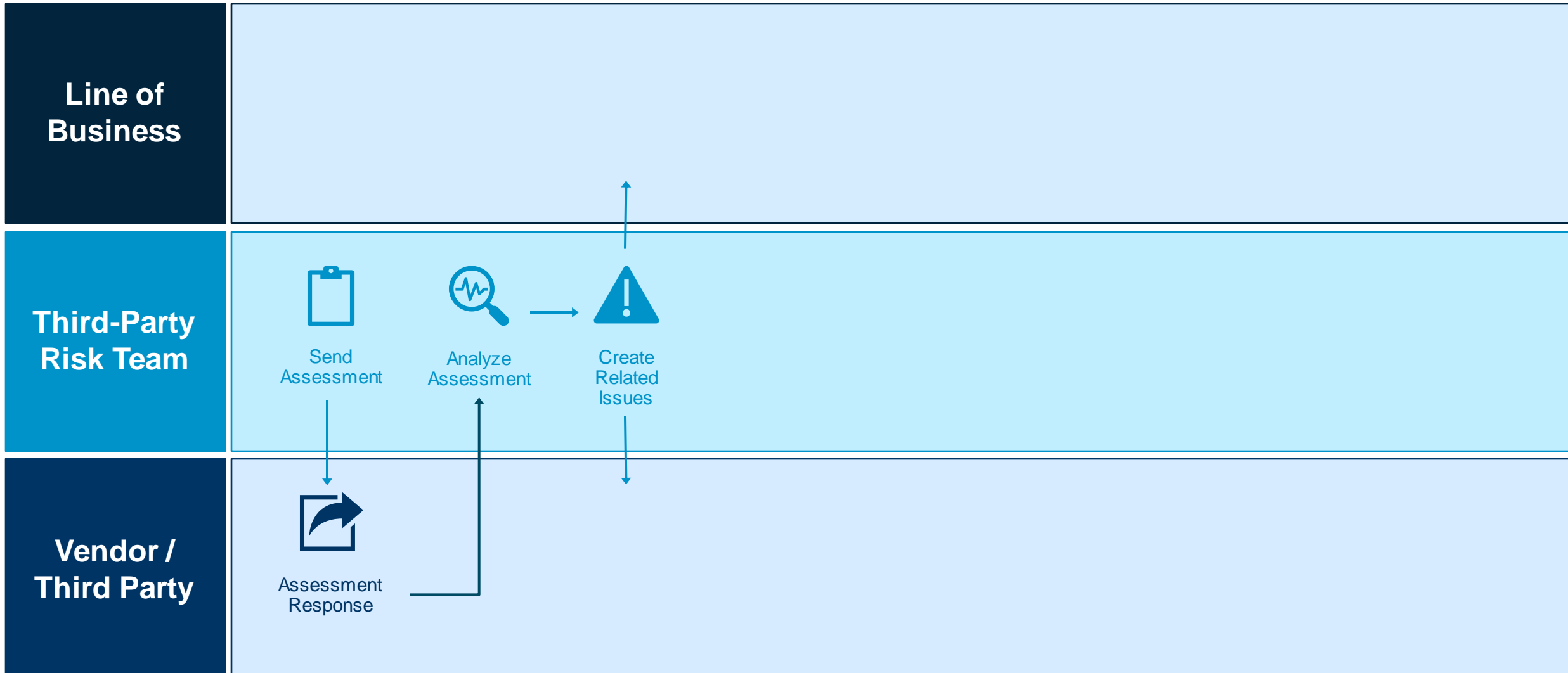
Ongoing Monitoring: Periodic Due Diligence



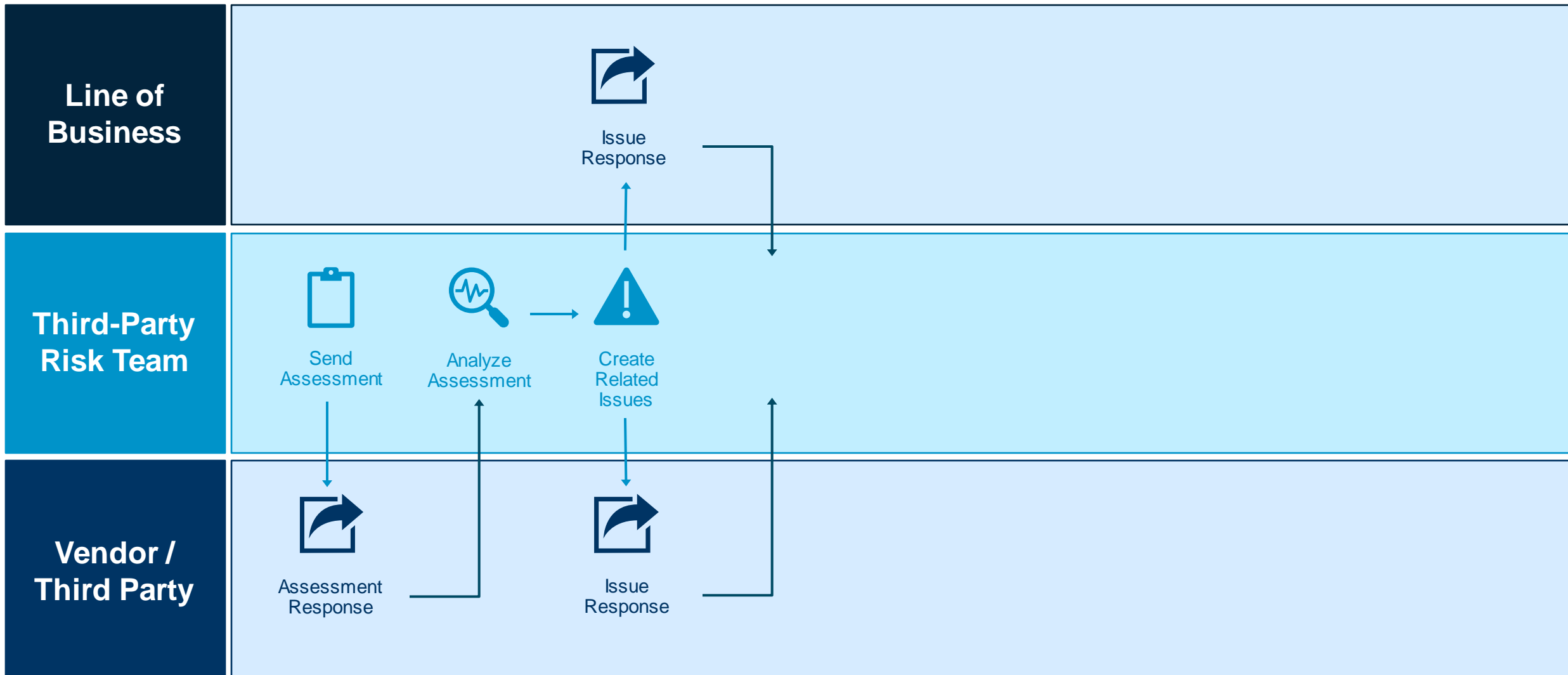
Ongoing Monitoring: Periodic Due Diligence



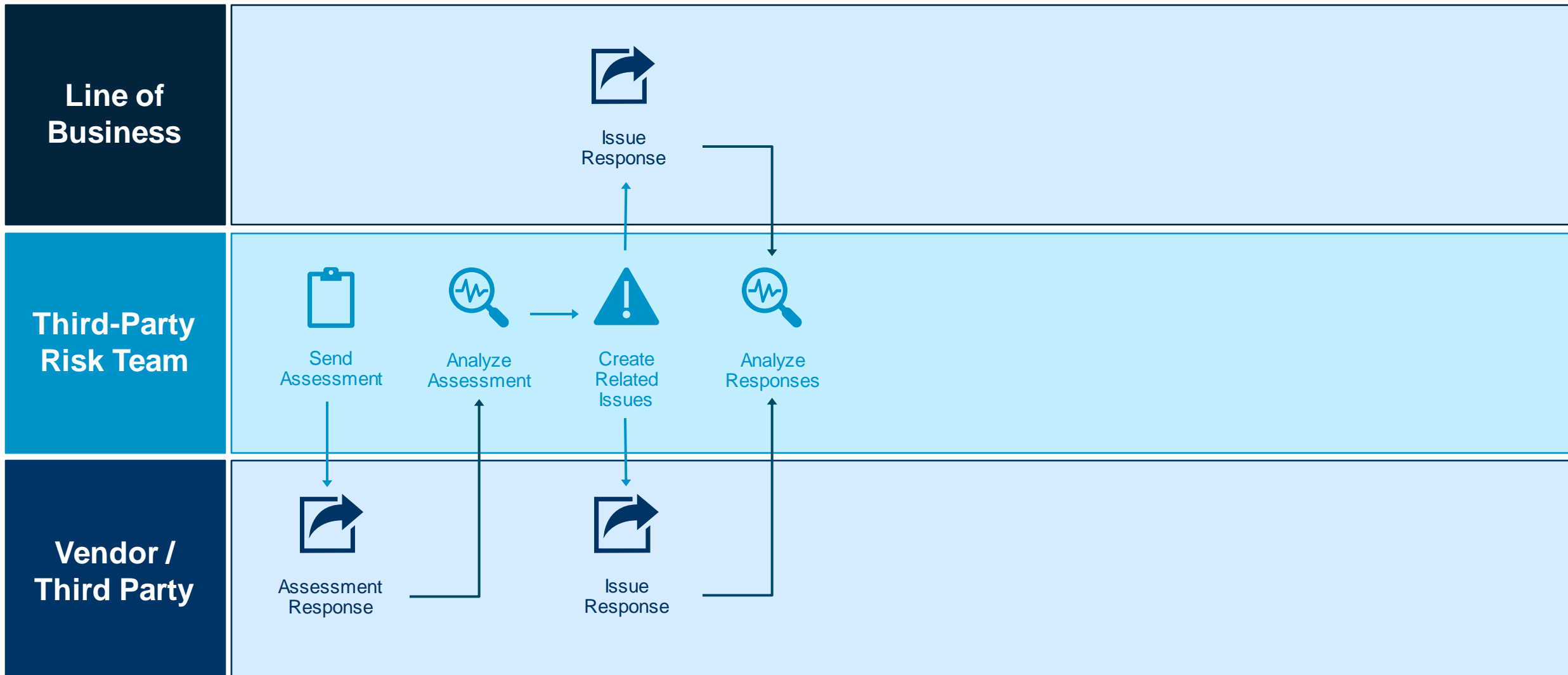
Ongoing Monitoring: Periodic Due Diligence



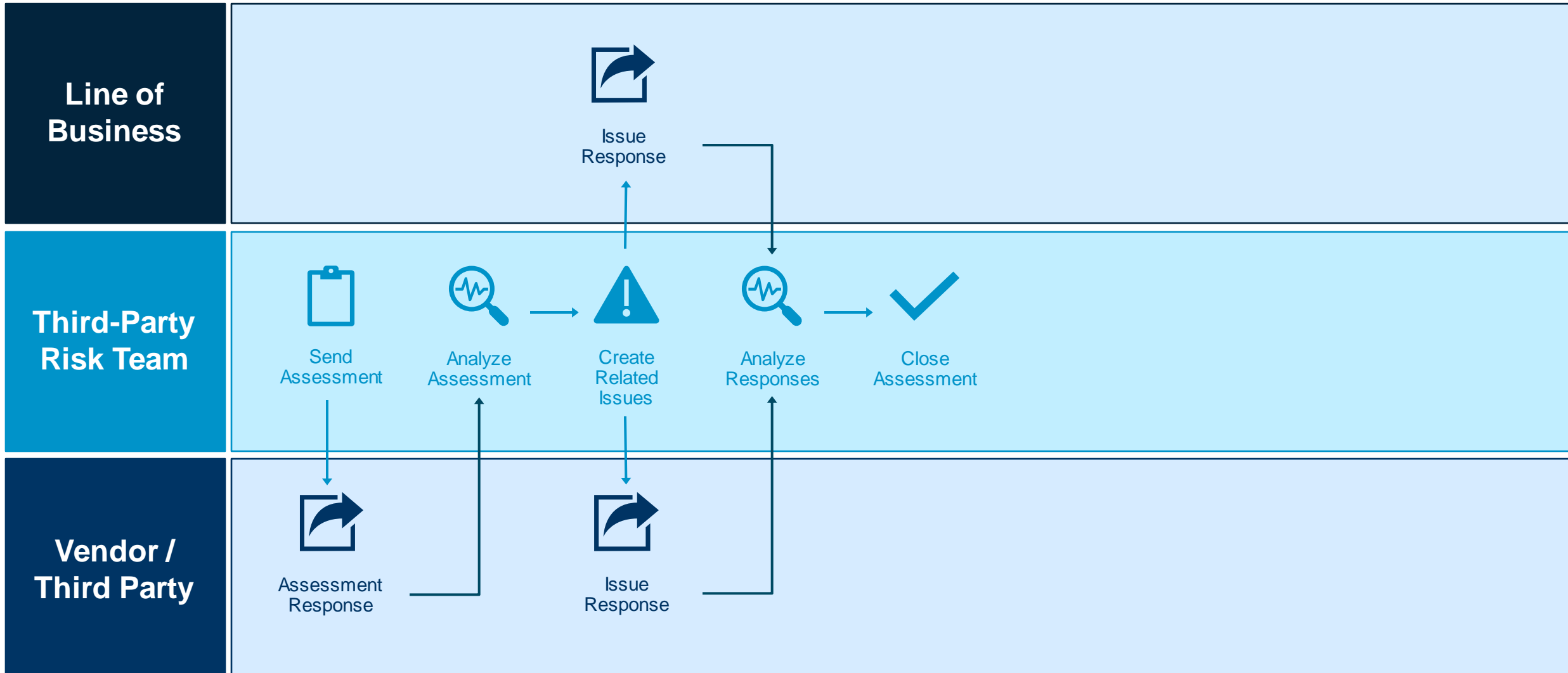
Ongoing Monitoring: Periodic Due Diligence



Ongoing Monitoring: Periodic Due Diligence



Ongoing Monitoring: Periodic Due Diligence

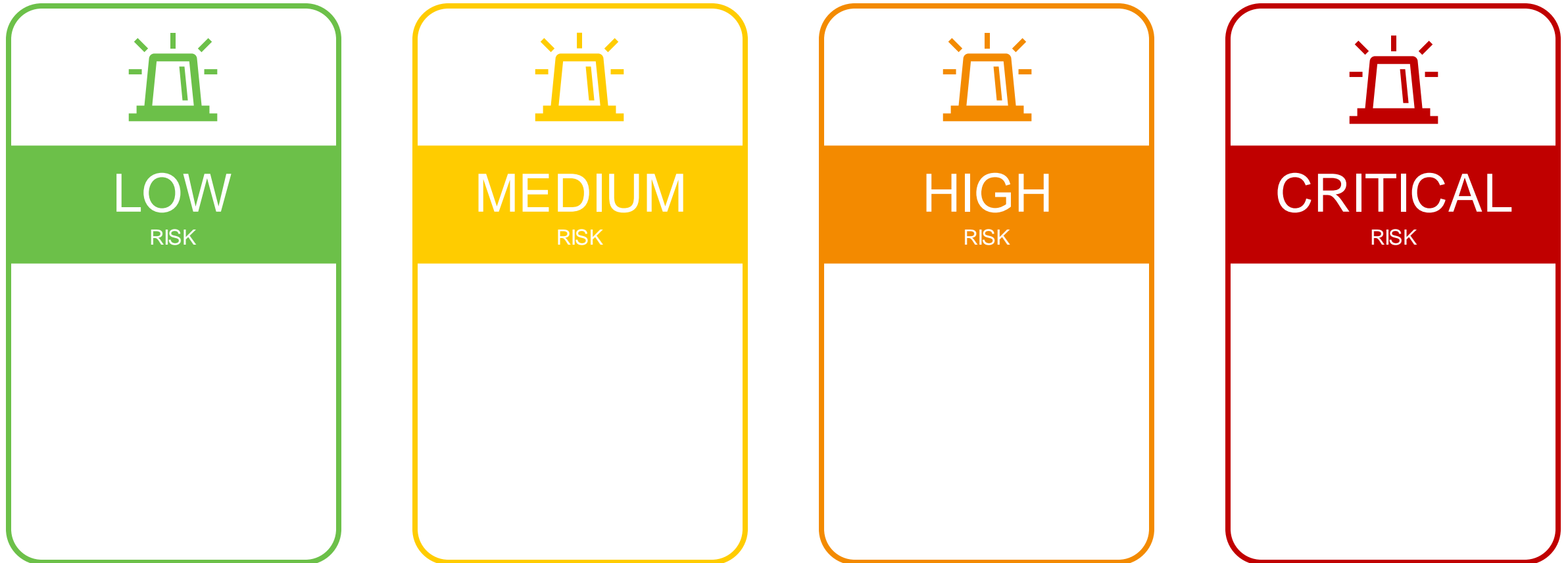


THIRD-PARTY RISK MANAGEMENT

Determining Scope & Frequency

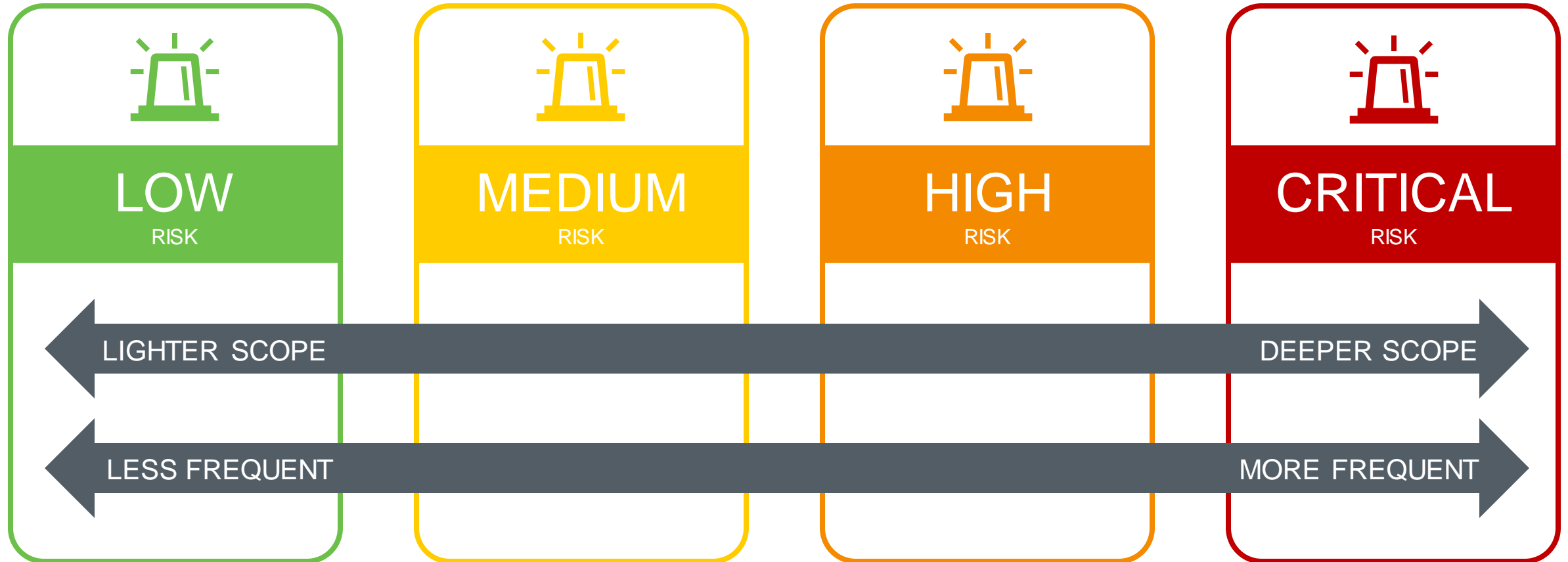
Scope & Frequency: The Basics

NOT ALL VENDORS WARRANT THE SAME LEVEL OF ATTENTION



Scope & Frequency: The Basics

NOT ALL VENDORS WARRANT THE SAME LEVEL OF ATTENTION



Scope & Frequency: The Basics

NOT ALL VENDORS WARRANT THE SAME LEVEL OF ATTENTION



LOW
RISK

- No or Infrequent Due Diligence



MEDIUM
RISK

- Light Due Diligence
- Biennially



HIGH
RISK

- Medium Due Diligence
- Annually



CRITICAL
RISK

- Heavy Due Diligence
- Annually

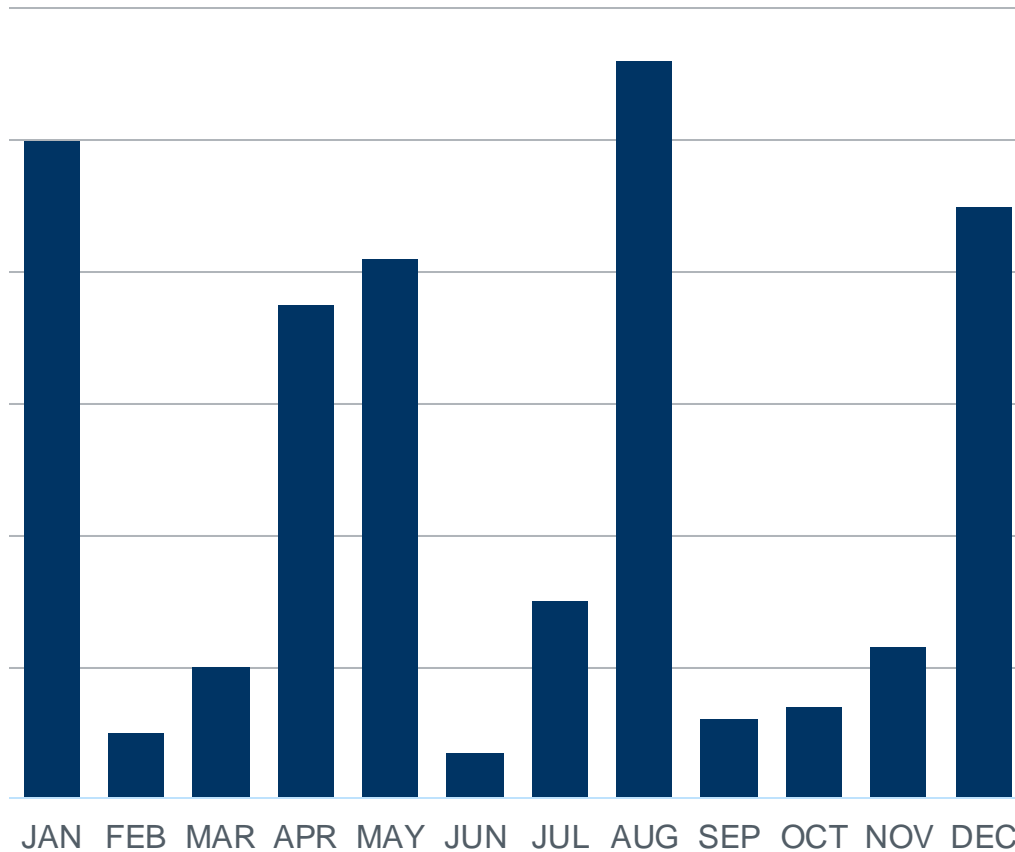
Tip: Be Smart with Scheduling

BALANCED ASSESSMENT SCHEDULES REDUCE BACKLOG RISK

Tip: Be Smart with Scheduling

BALANCED ASSESSMENT SCHEDULES REDUCE BACKLOG RISK

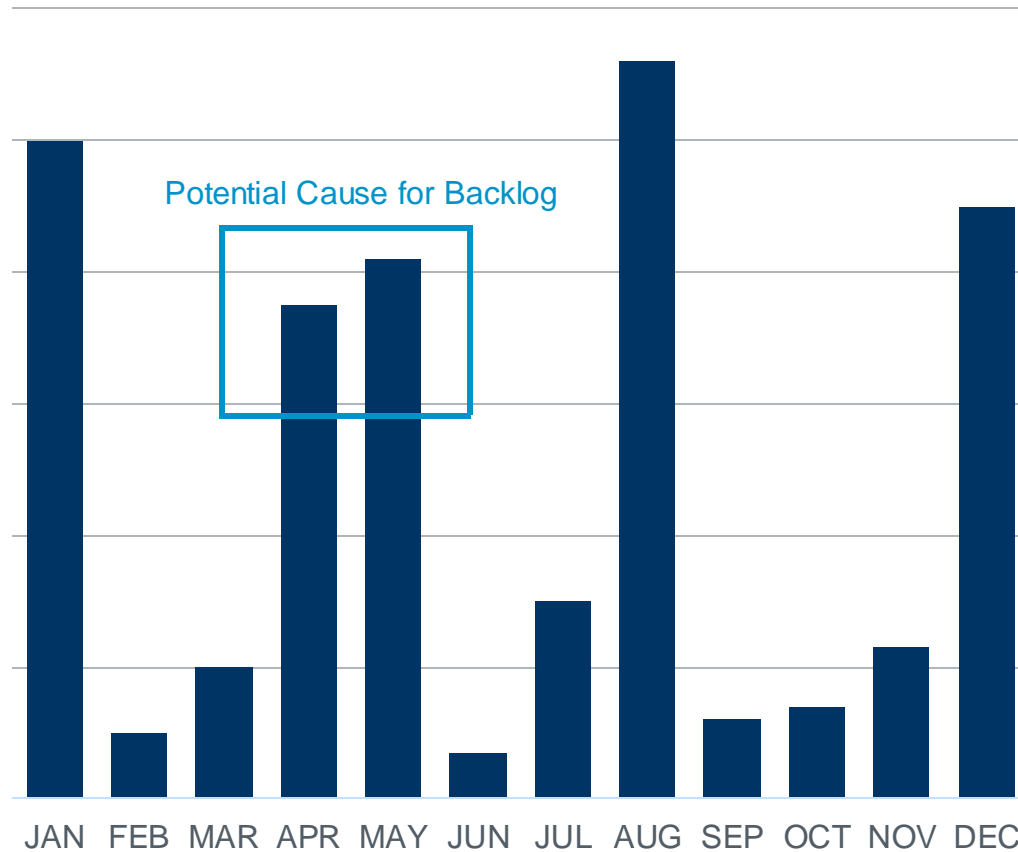
Unbalanced Schedule



Tip: Be Smart with Scheduling

BALANCED ASSESSMENT SCHEDULES REDUCE BACKLOG RISK

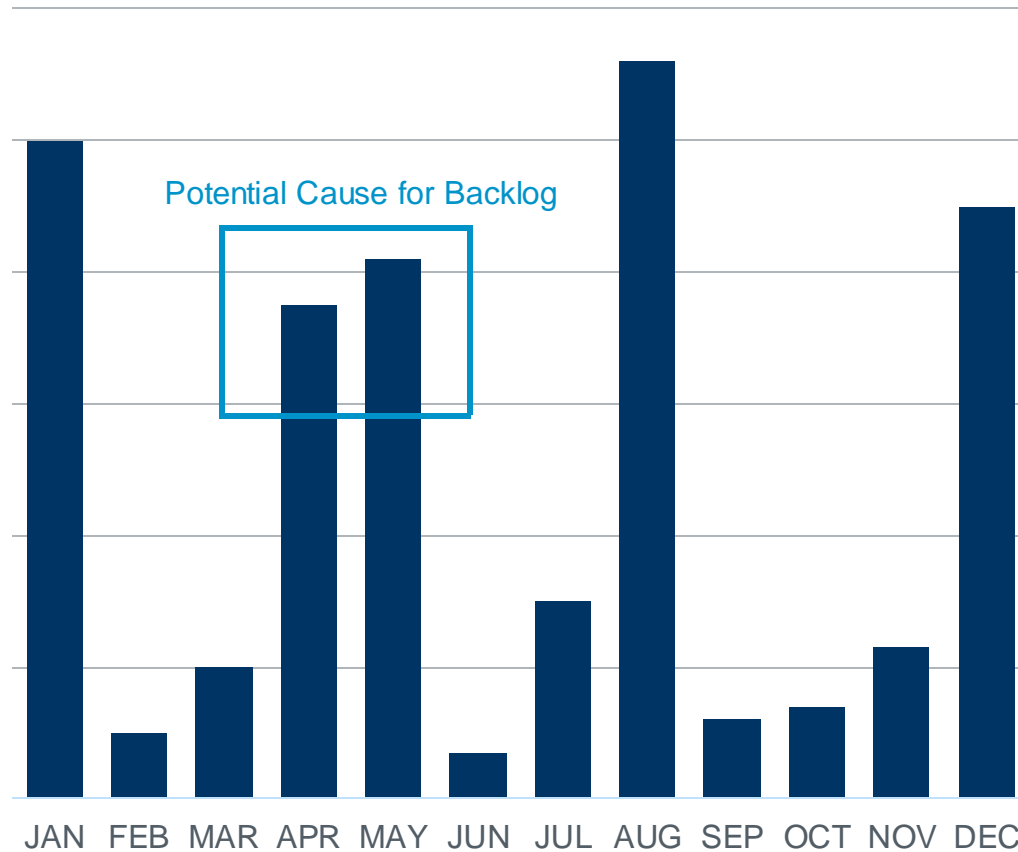
Unbalanced Schedule



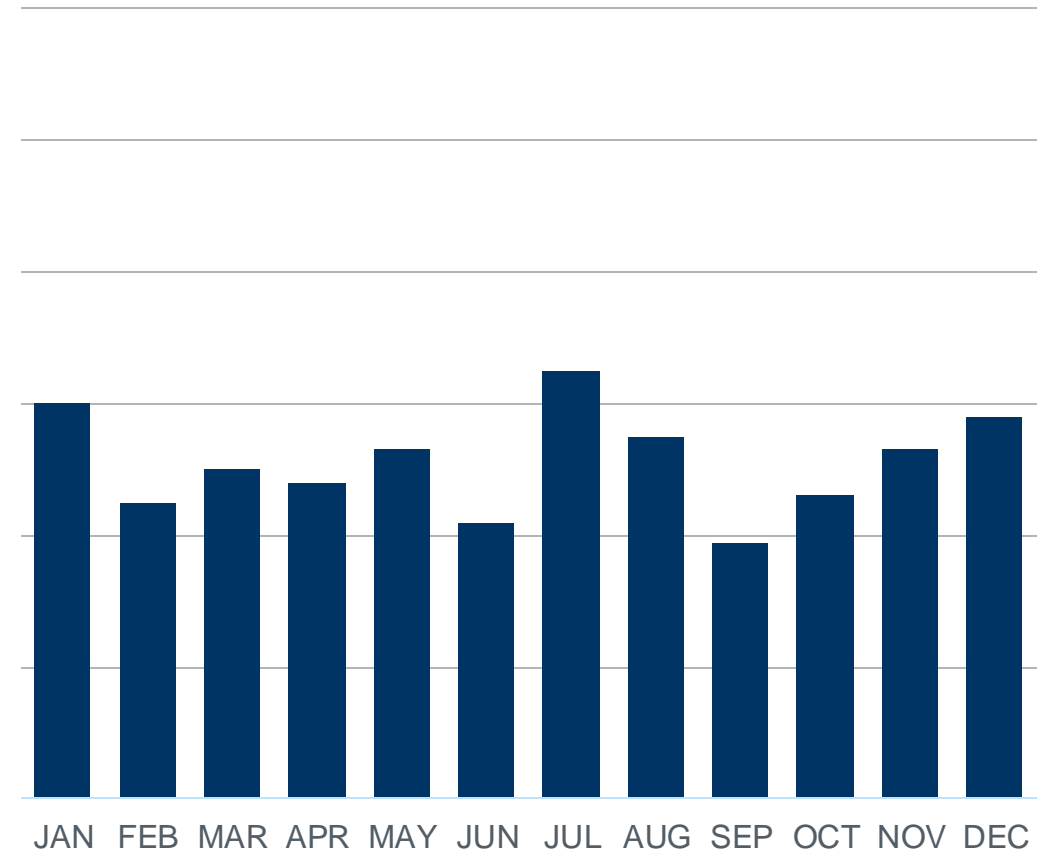
Tip: Be Smart with Scheduling

BALANCED ASSESSMENT SCHEDULES REDUCE BACKLOG RISK

Unbalanced Schedule



Balanced Schedule



Tip: Relieve Backlog via Outsourcing

REDUCE BACKLOG, ASSESS “HARD-TO-ASSESS” VENDORS, ACCESS SUBJECT-MATTER EXPERTS

Assessments
as a Service

 **accenture**

 **CastleHill**
MANAGED RISK SOLUTIONS

 **Crowe**

 **Cybersel**

Deloitte.

 **DVV** solutions

 **EY**

 **genpact**

 **GUIDEPOINT**
SECURITY

HCL

Next-Level: Inherent Risk Drives Schedule & Scope

Next-Level: Inherent Risk Drives Schedule & Scope



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

Next-Level: Inherent Risk Drives Schedule & Scope

Inherent Risk

Previous Assessment Rating

Next-Level: Inherent Risk Drives Schedule & Scope

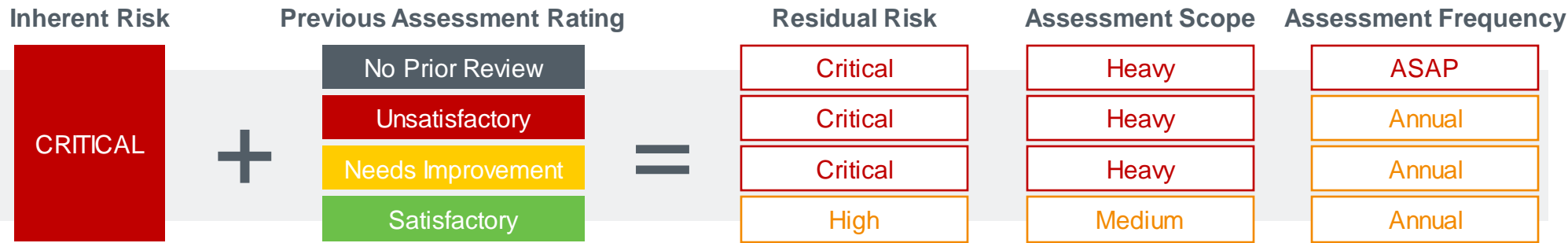
Inherent Risk



Previous Assessment Rating



Next-Level: Inherent Risk Drives Schedule & Scope



Next-Level: Inherent Risk Drives Schedule & Scope

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	None	N/A
		Unsatisfactory		Low	None	N/A
		Needs Improvement		Low	None	N/A
		Satisfactory		Low	None	N/A

THIRD-PARTY RISK MANAGEMENT

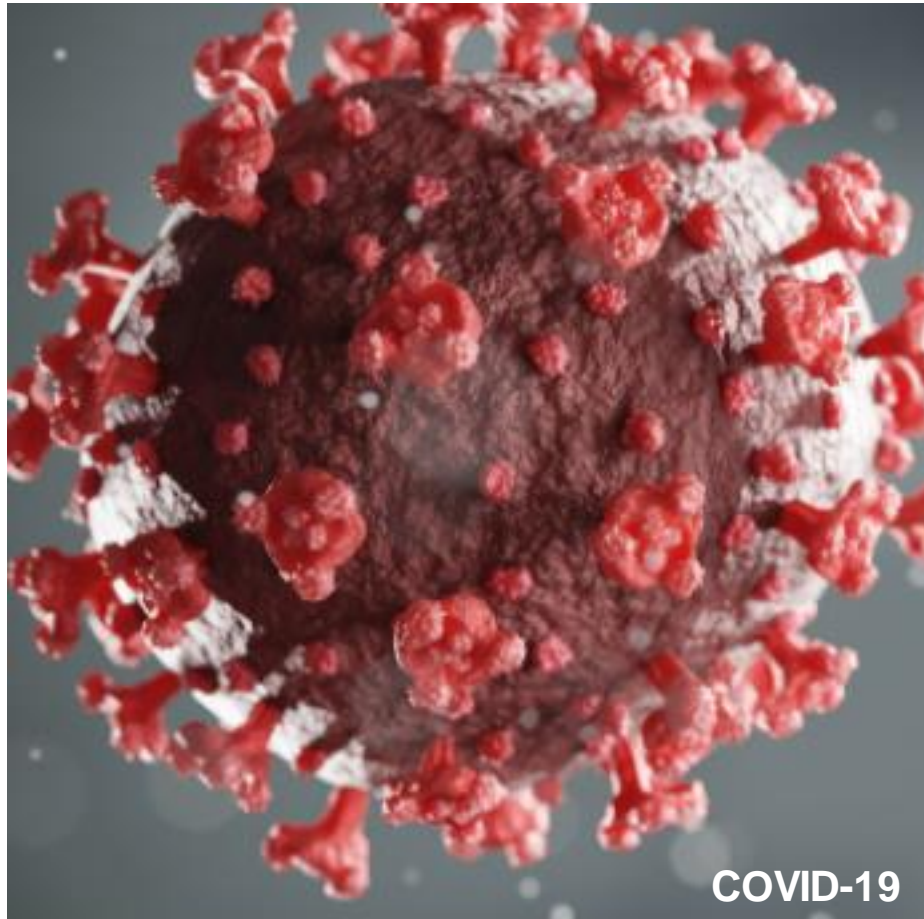
Be Prepared for Unexpected Changes to the Schedule

Emerging Risks Require Agility

BE PREPARED FOR UNEXPECTED BREAKS IN THE NORMAL REVIEW CYCLE

Emerging Risks Require Agility

BE PREPARED FOR UNEXPECTED BREAKS IN THE NORMAL REVIEW CYCLE



“Emergency-Use” Questionnaires

The screenshot displays a web application titled "Pandemic Assessment". The interface includes a top navigation bar with icons for mail, clock, checkmark, and settings. A left sidebar contains a list of questions, some of which are checked. The main content area on the right shows a detailed view of four specific questions:

- **PQ5:** Where are your greatest geographic concentrations of product/service delivery?
- **PQ6:** Where are your greatest geographic concentrations of third parties (our fourth parties)?
- **PQ7:** Are you able to deliver the product/service via a remote workforce?
- **PQ8:** Are you initiating work-from-home policies for personnel involved in delivering the product or service?

Tip: Prepare Question Sets in Advance

REDUCE REACTION TIME & EMPLOY HIGHER QUALITY QUESTIONNAIRES

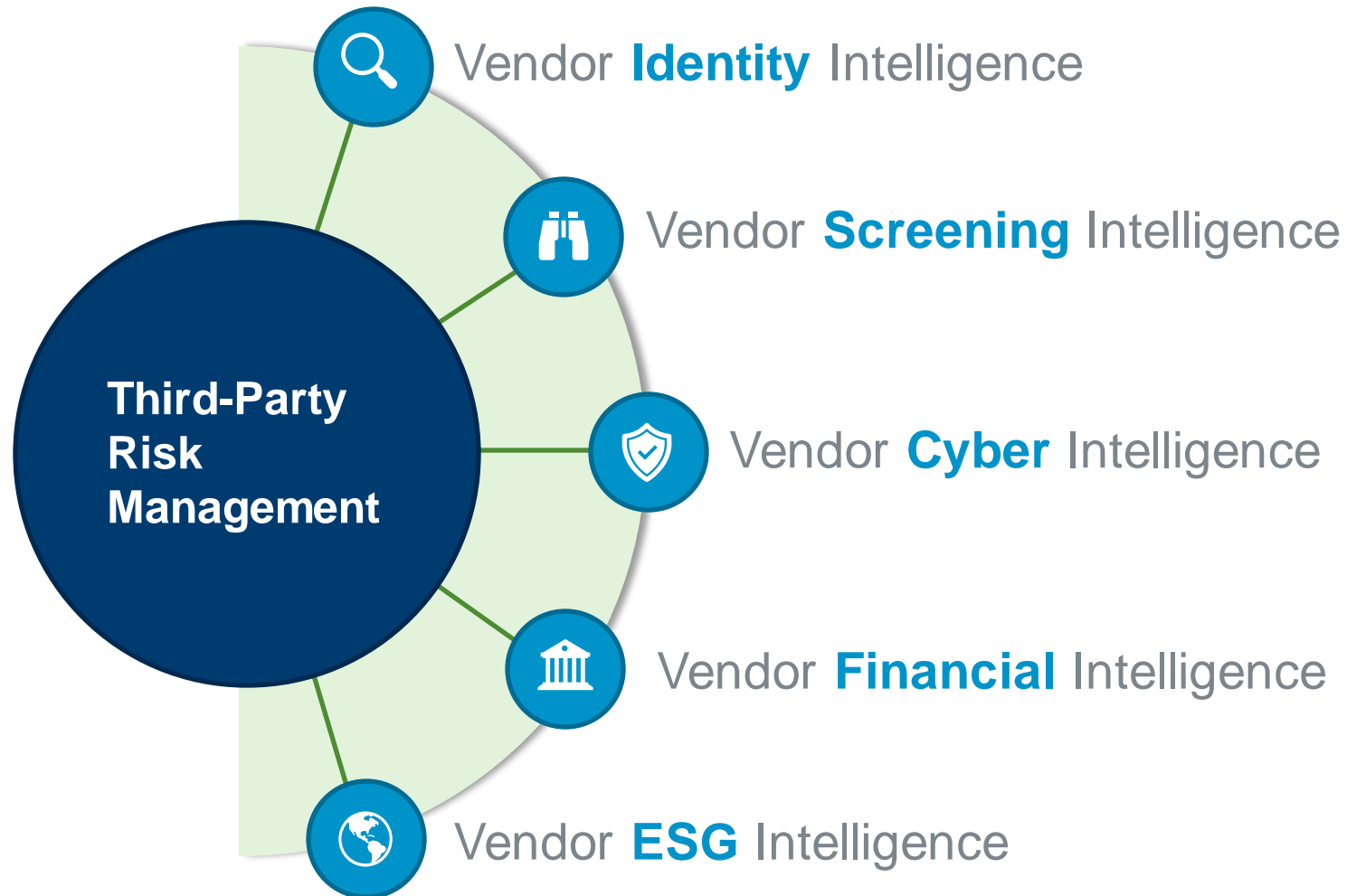


THIRD-PARTY RISK MANAGEMENT

Incorporate Expert Vendor Intelligence into Monitoring Processes

Expert Vendor Intelligence

ENRICH THIRD-PARTY RISK LIFECYCLE PROCESSES WITH TARGETED RISK INTELLIGENCE



Capture Holistic Risk Postures & Streamline Third-Party Reviews

- More accurate onboarding via targeted embedded ratings
- Deeper due diligence based on specific risk domains
- Automated monitoring between periodic vendor assessments
- Automated issue identification and creation
- Streamlined reporting by risk domain for visibility across vendor population

Expert Vendor Intelligence

- Cybersecurity Ratings:
 - BitSight
 - RiskRecon
 - SecurityScorecard
- Financial Health Scores:
 - Rapid Ratings
 - Dun & Bradstreet
- Environmental, Social, Governance
 - EcoVadis
- ABAC / UBO
 - Refinitiv
- Negative News Feeds
 - Refinitiv
- 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
Refinitiv WC1 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
Refinitiv WC1 Positive Results: 2
EcoVadis Ethics Score: 30

Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE

Continuously Scan for Material Changes

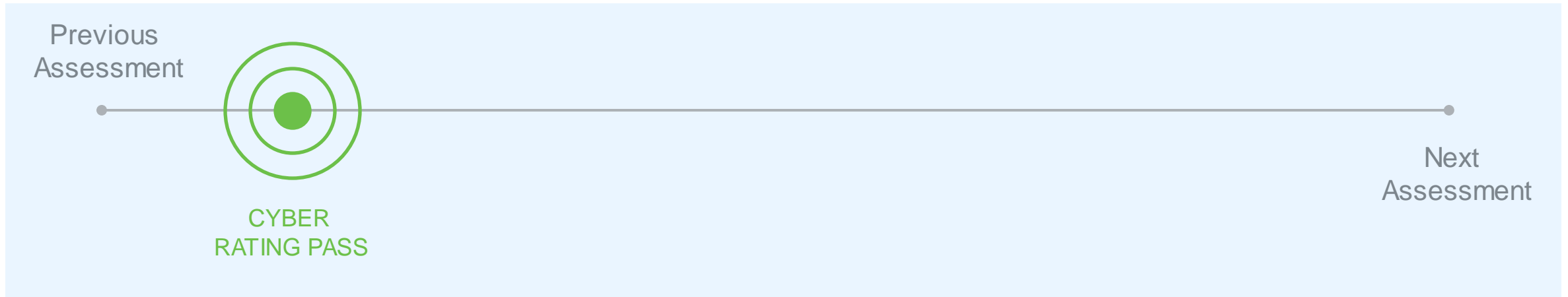
EXPERT VENDOR INTELLIGENCE

Previous
Assessment

Next
Assessment

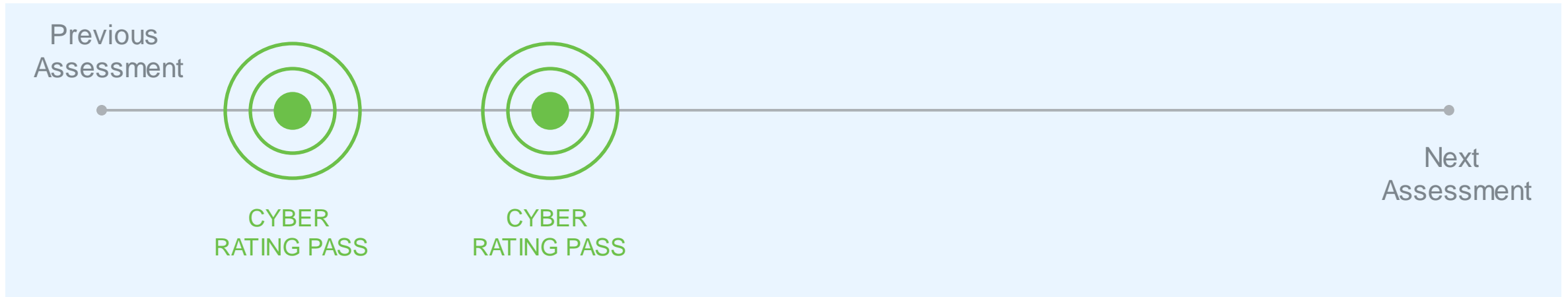
Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



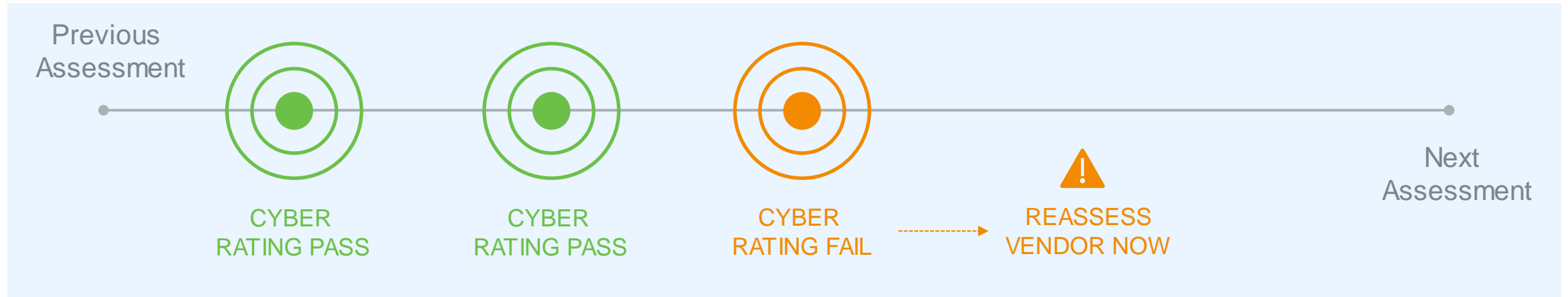
Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



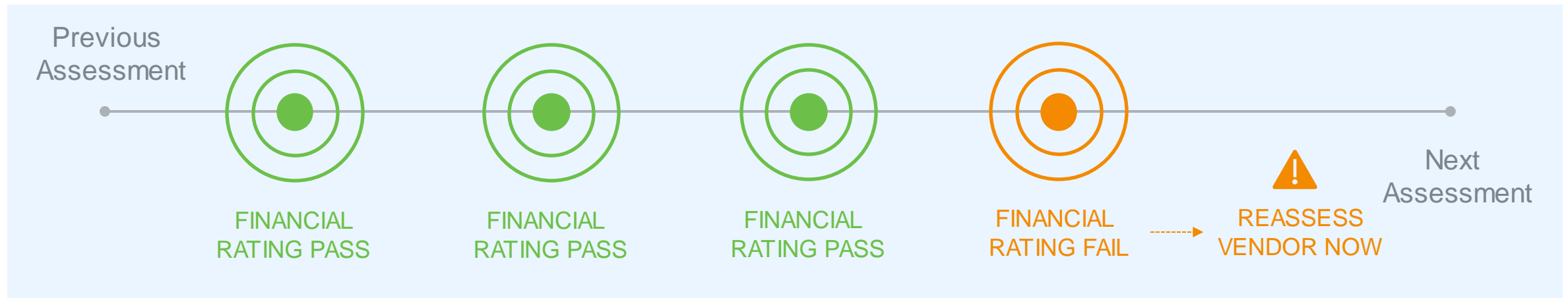
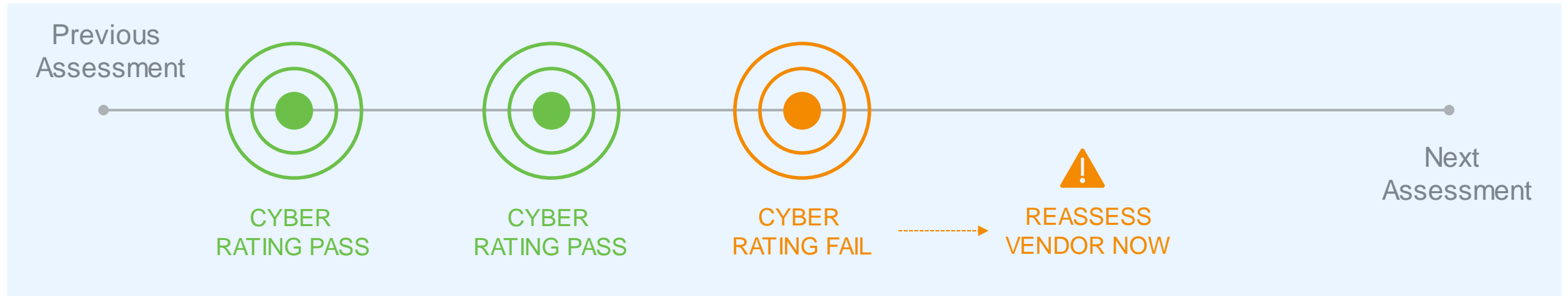
Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE



Continuously Scan for Material Changes

EXPERT VENDOR INTELLIGENCE

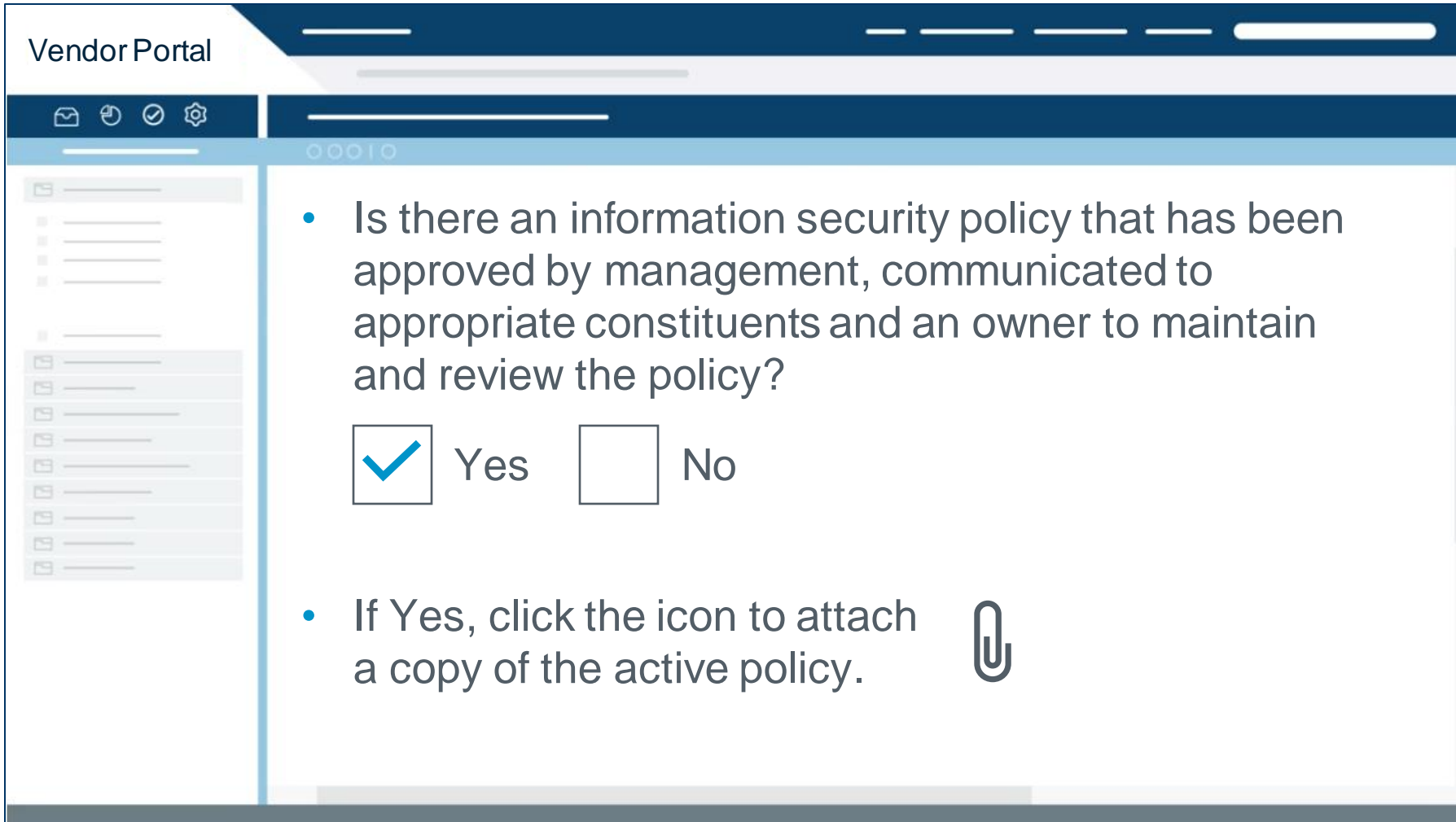


THIRD-PARTY RISK MANAGEMENT

Reduce Vendor Fatigue (to Improve Results)


Tip: Take Steps to Reduce Vendor Fatigue

DOCUMENTATION MANAGEMENT



The screenshot shows a web application titled "Vendor Portal". It features a dark blue header with navigation icons (mail, clock, checkmark, gear) and a sidebar with a list of items. The main content area displays a questionnaire with two questions. The first question asks if there is an information security policy approved by management, with "Yes" selected. The second question asks to attach a copy of the active policy, with a paperclip icon provided for attachment.

Vendor Portal

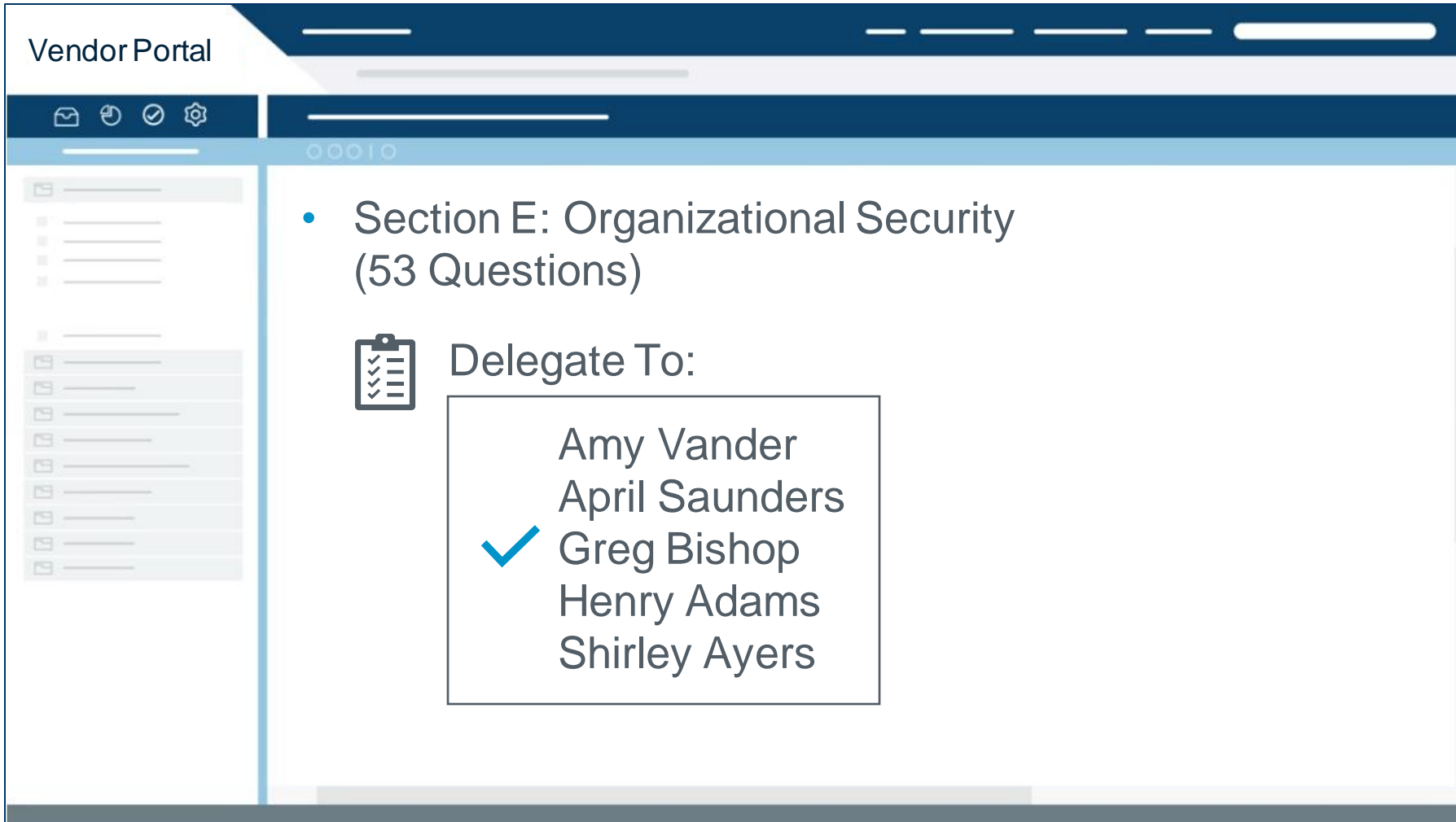
- Is there an information security policy that has been approved by management, communicated to appropriate constituents and an owner to maintain and review the policy?
☒ Yes ☐ No
- If Yes, click the icon to attach a copy of the active policy. 

Allow vendors to associate policies, documents and supporting evidence with specific questions.

Next-Level: Allow documents to be associated with multiple question responses.

Tip: Take Steps to Reduce Vendor Fatigue

QUESTIONNAIRE DELEGATION



The screenshot shows a web application titled "Vendor Portal". On the left is a sidebar with a list of questionnaire sections. The main content area displays "Section E: Organizational Security (53 Questions)". Below this, there is a "Delegate To:" section with a clipboard icon. A list of names is shown, with a blue checkmark next to "Greg Bishop".

Vendor Portal

Section E: Organizational Security (53 Questions)

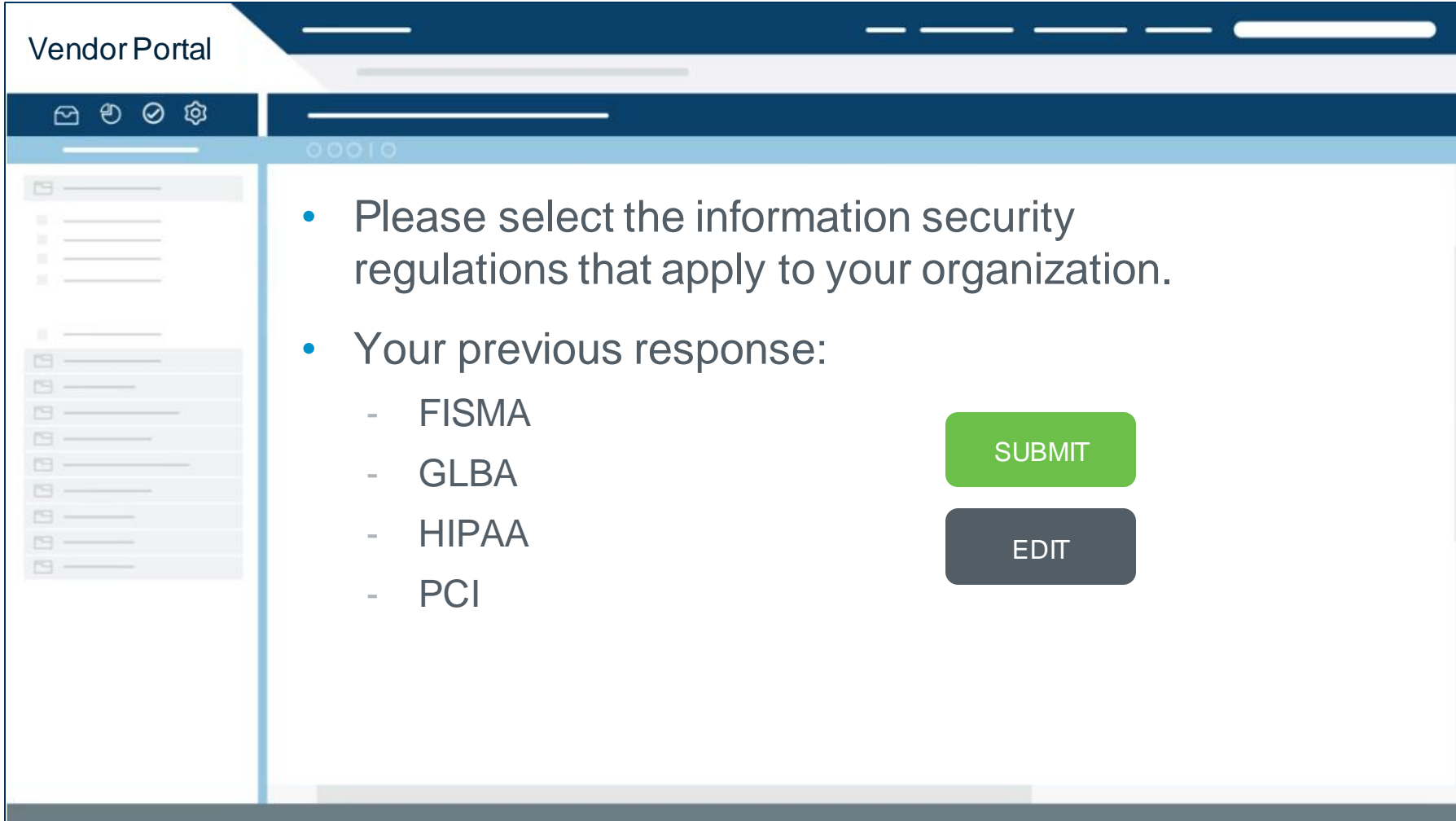
Delegate To:

- Amy Vander
- April Saunders
- ✓ Greg Bishop
- Henry Adams
- Shirley Ayers

Allow vendors to delegate questions or groups of questions to subject matter experts within their organization.

Tip: Take Steps to Reduce Vendor Fatigue

UPDATE / CONFIRM PREVIOUS ASSESSMENT RESPONSES



The screenshot shows a 'Vendor Portal' interface. On the left is a sidebar with a list of items, some with checkboxes. The main content area displays two bullet points: 'Please select the information security regulations that apply to your organization.' and 'Your previous response:'. Below the second bullet point is a list of regulations: FISMA, GLBA, HIPAA, and PCI. To the right of this list are two buttons: a green 'SUBMIT' button and a grey 'EDIT' button.

- Please select the information security regulations that apply to your organization.
- Your previous response:
 - FISMA
 - GLBA
 - HIPAA
 - PCI

SUBMIT

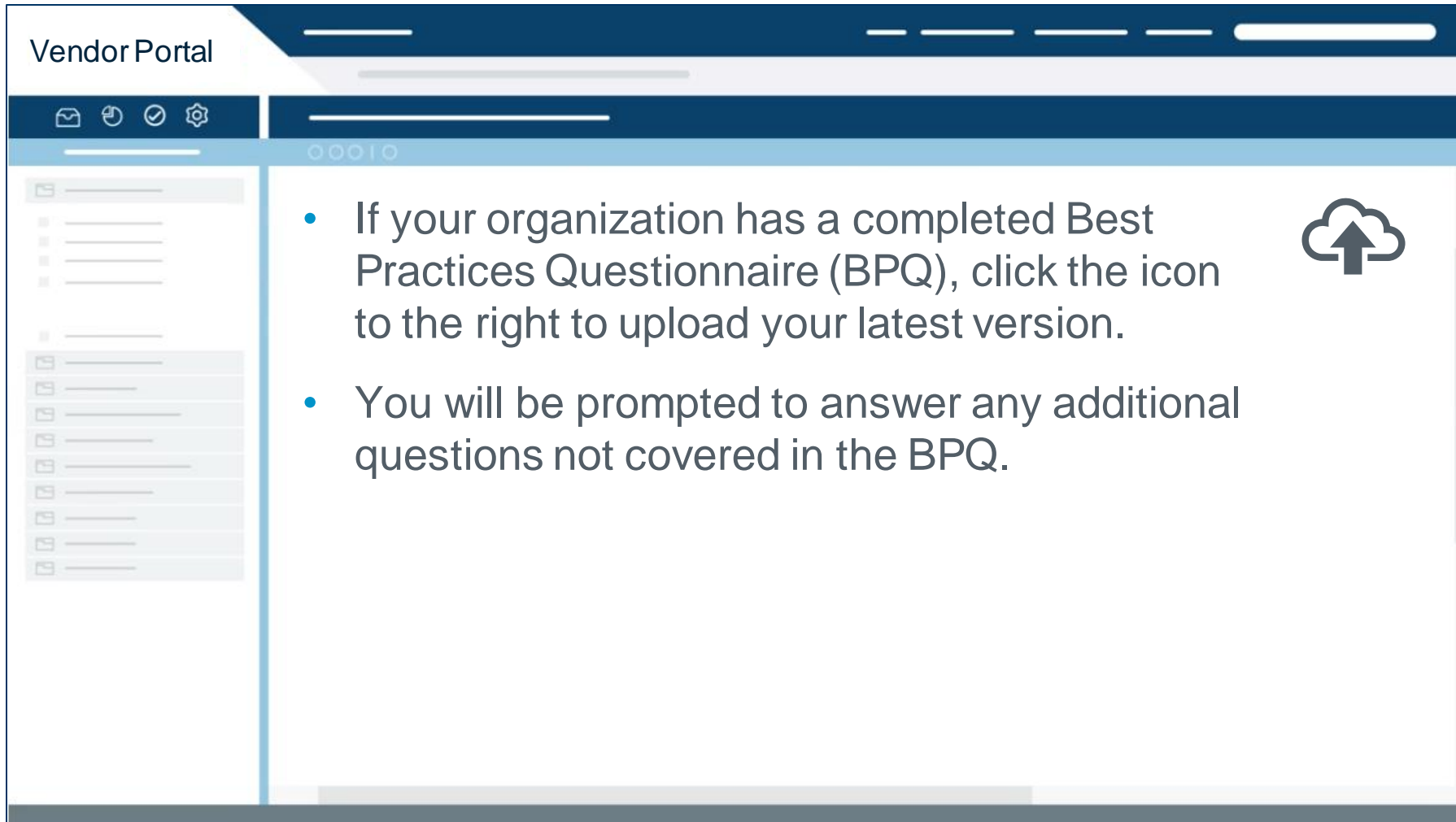
EDIT

Provide vendors with their answers from their most recent assessment to speed response time.

Caution: Sometimes “easier” for the vendor is not ideal for risk reduction. Consider which questions to provide previous answers.

Tip: Take Steps to Reduce Vendor Fatigue

INGEST INDUSTRY-STANDARD QUESTIONNAIRES



Allow vendors to submit their completed industry-standard questionnaire.

Next-Level: Map vendor responses to your questionnaire and ask the vendor to complete the unmapped questions.

THIRD-PARTY RISK MANAGEMENT

Next-Level: Renewals,
Service Reviews, SLAs
& More...

Incorporating Key Processes into Monitoring Activities



Onboarding

Establish an enterprise-wide process



Due Diligence

Enforce objectivity within your vendor process



Ongoing Monitoring

Streamline processes while reducing errors



On-Site Control Assessment

Systematically conduct and document



Performance Reviews

Manage with consistency



Contract Reviews

Create a unified process



SLA Monitoring

Document, monitor and record



Issue Management

Formally track vendor issues

Incorporating Key Processes into Monitoring Activities



Onboarding

Establish an enterprise-wide process



Due Diligence

Enforce objectivity within your vendor process



Ongoing Monitoring

Streamline processes while reducing errors



On-Site Control Assessment

Systematically conduct and document



Performance Reviews

Manage with consistency



Contract Reviews

Create a unified process



SLA Monitoring

Document, monitor and record

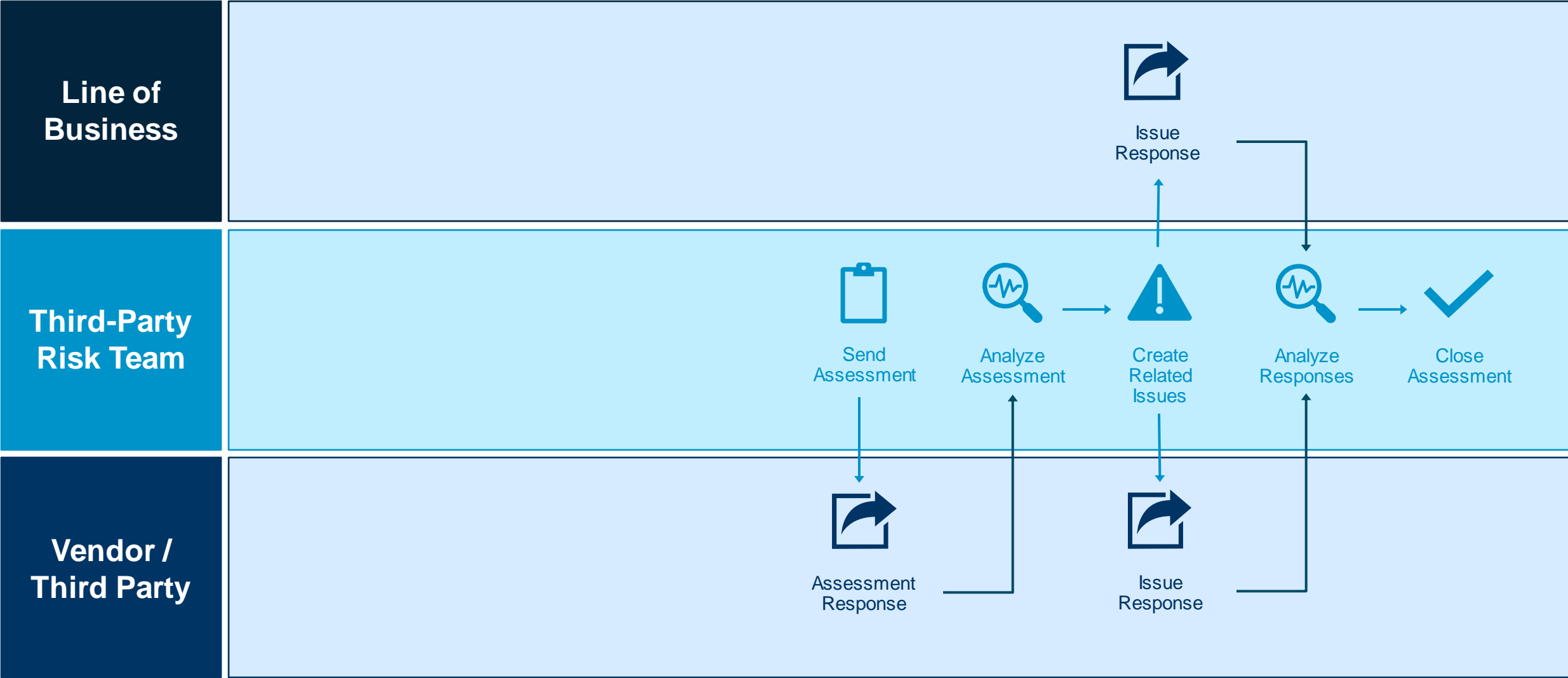


Issue Management

Formally track vendor issues

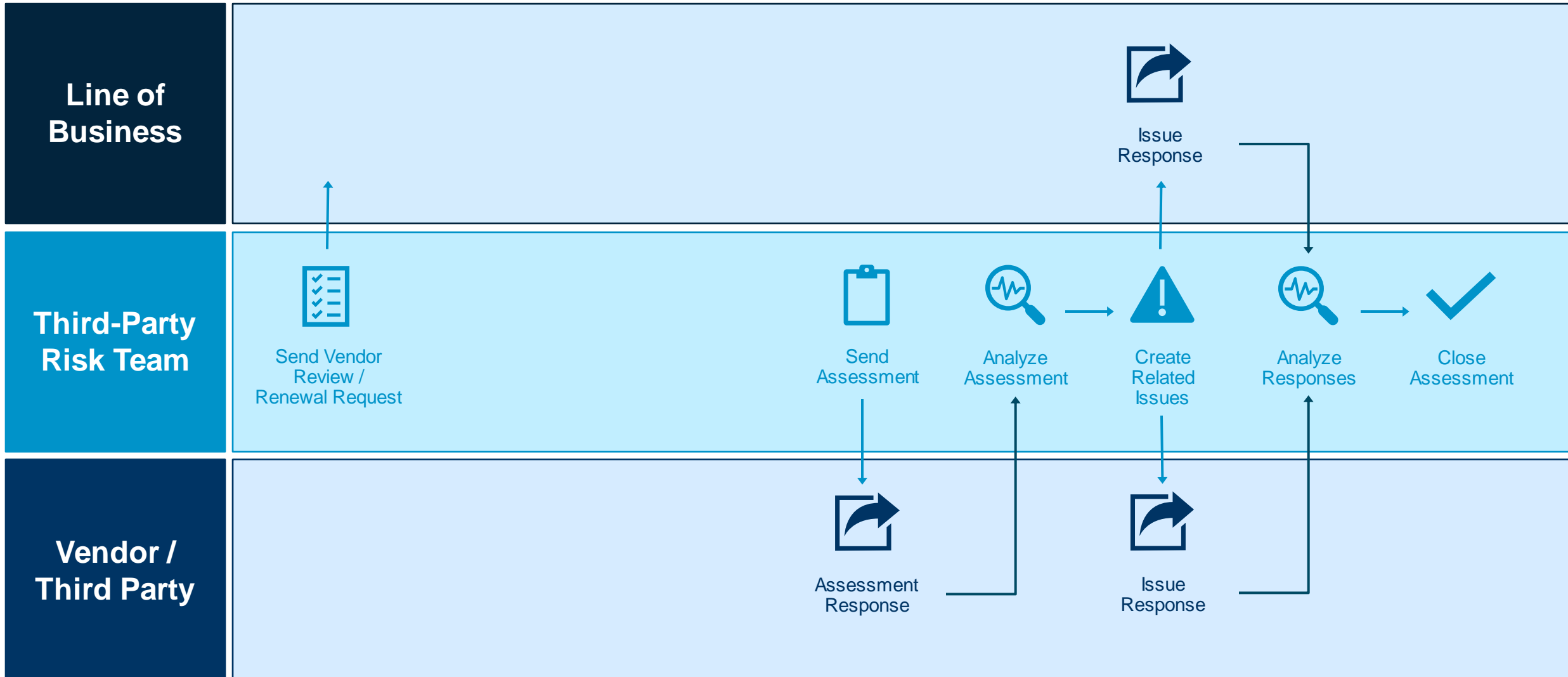
Next-Level: Involve Line-of-Business in Due Diligence

INCORPORATE RENEWALS & REVIEWS IN CONJUNCTION WITH PERIODIC ASSESSMENTS



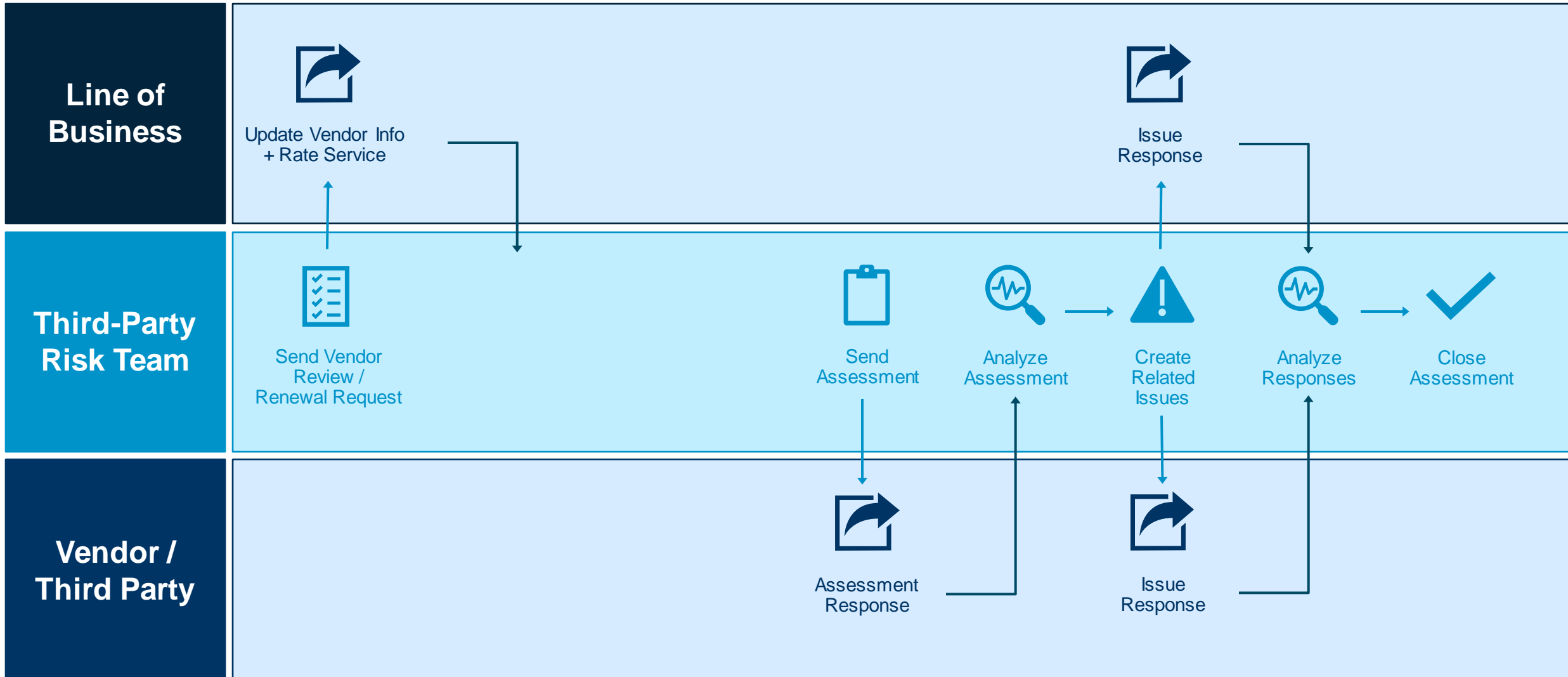
Next-Level: Involve Line-of-Business in Due Diligence

INCORPORATE RENEWALS & REVIEWS IN CONJUNCTION WITH PERIODIC ASSESSMENTS



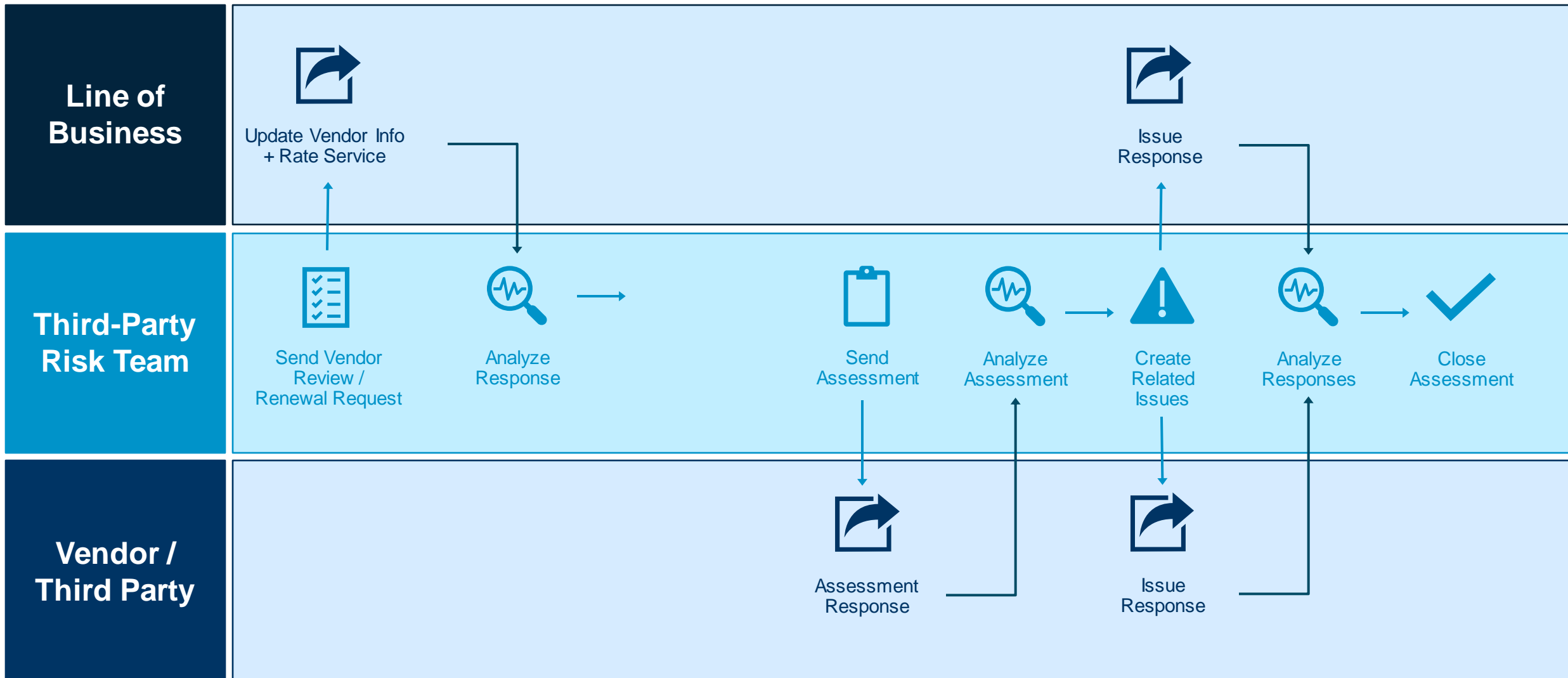
Next-Level: Involve Line-of-Business in Due Diligence

INCORPORATE RENEWALS & REVIEWS IN CONJUNCTION WITH PERIODIC ASSESSMENTS



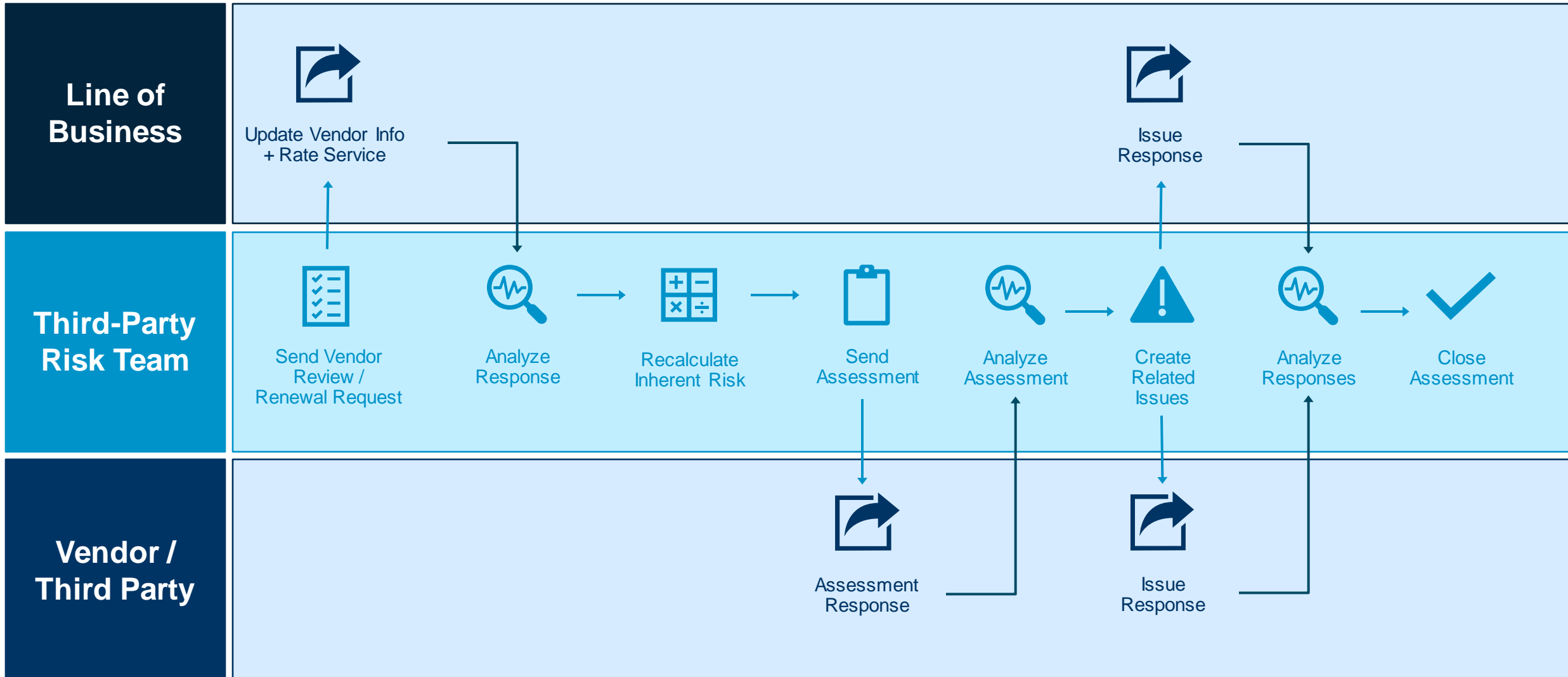
Next-Level: Involve Line-of-Business in Due Diligence

INCORPORATE RENEWALS & REVIEWS IN CONJUNCTION WITH PERIODIC ASSESSMENTS



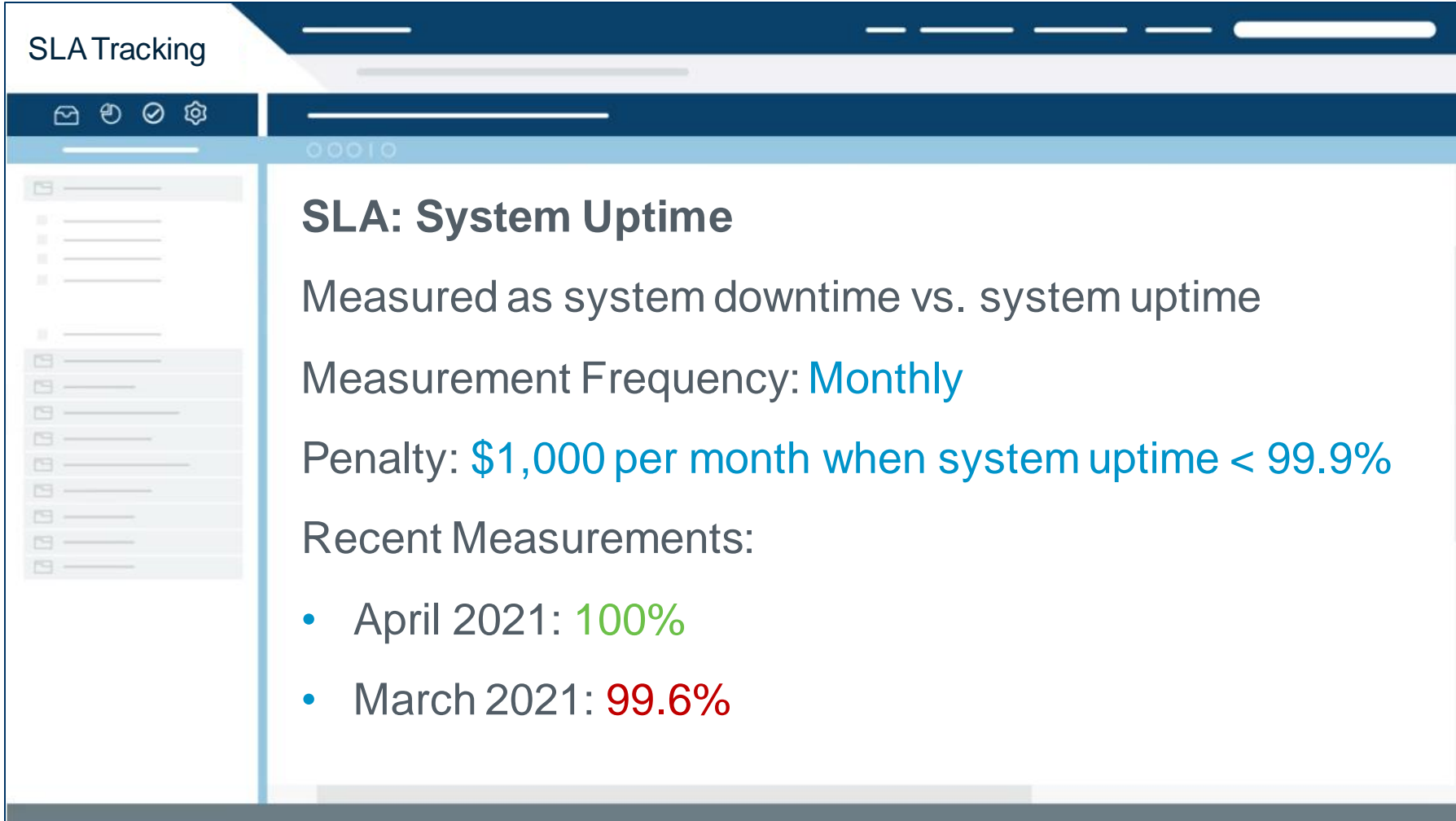
Next-Level: Involve Line-of-Business in Due Diligence

INCORPORATE RENEWALS & REVIEWS IN CONJUNCTION WITH PERIODIC ASSESSMENTS



Next-Level: Review & Track SLAs

REVIEW SLAS WITH LOB VENDOR OWNERS DURING REVIEW PERIODS



The screenshot shows a web application titled "SLA Tracking". It features a dark blue header with navigation icons (envelope, clock, checkmark, gear) and a sidebar with a list of items. The main content area displays details for an "SLA: System Uptime".

SLA: System Uptime

Measured as system downtime vs. system uptime

Measurement Frequency: **Monthly**

Penalty: **\$1,000 per month when system uptime < 99.9%**

Recent Measurements:

- April 2021: **100%**
- March 2021: **99.6%**

Build a library of Service-Level Agreement types and measure vendors against them.

Use the ongoing monitoring schedule to review SLA performance.


Next-Level: Preferred Assessment Responses

QUICKLY IDENTIFY PROBLEM AREAS THAT REQUIRE ADDITIONAL SCRUTINY

Vendor Analysis


SO8: Does your organization have a formal Information Security policy?

Yes



SO9: Please select the option that best describes your incident detection and response practices and capabilities.

A. An incident Response Policy Exists

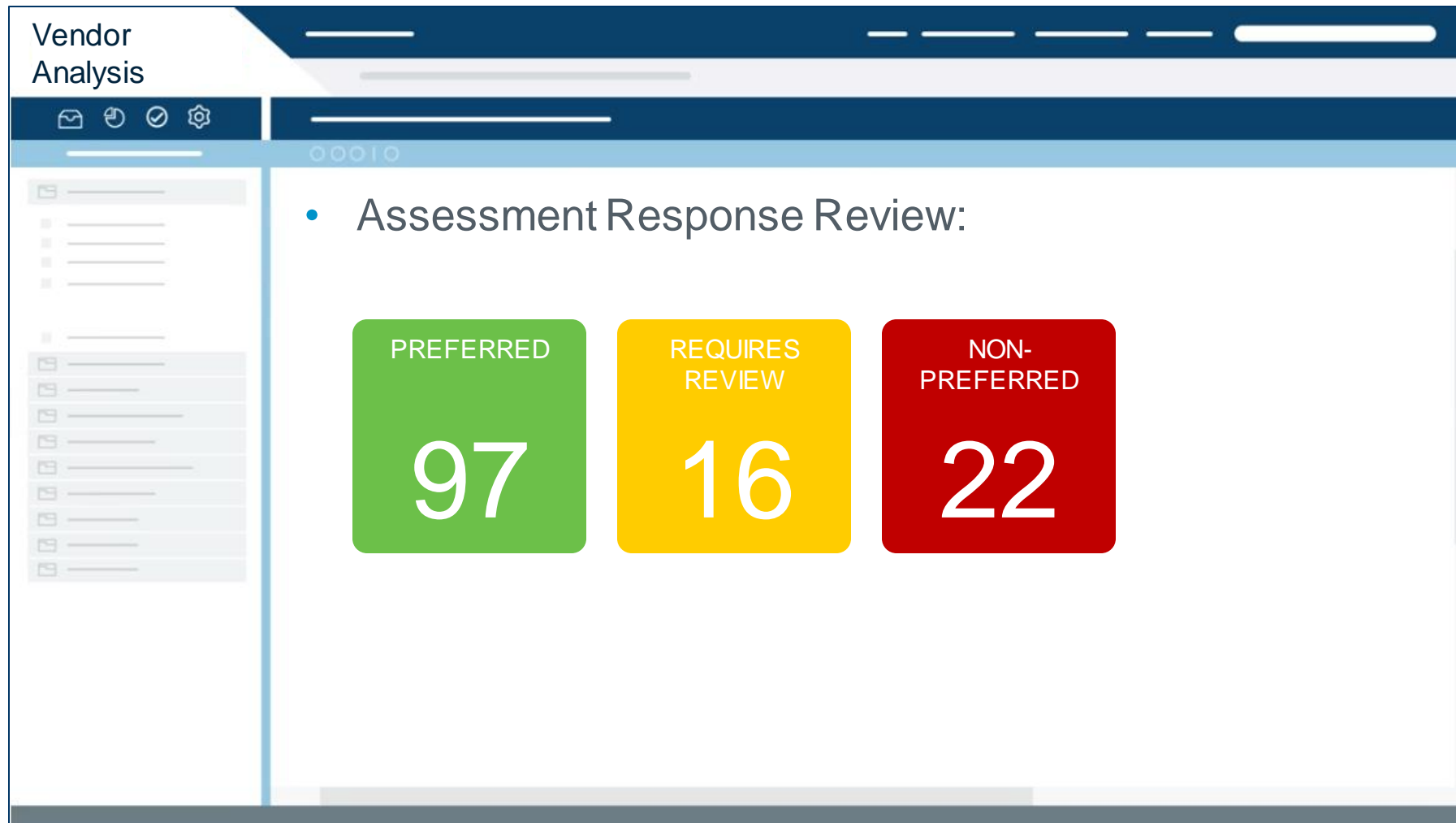


Design question sets with preferred responses that point analysts directly to potential problems.

Next-Level: Automatically generate tickets for issues identified via non-preferred responses.

Next-Level: Preferred Assessment Responses

QUICKLY IDENTIFY PROBLEM AREAS THAT REQUIRE ADDITIONAL SCRUTINY

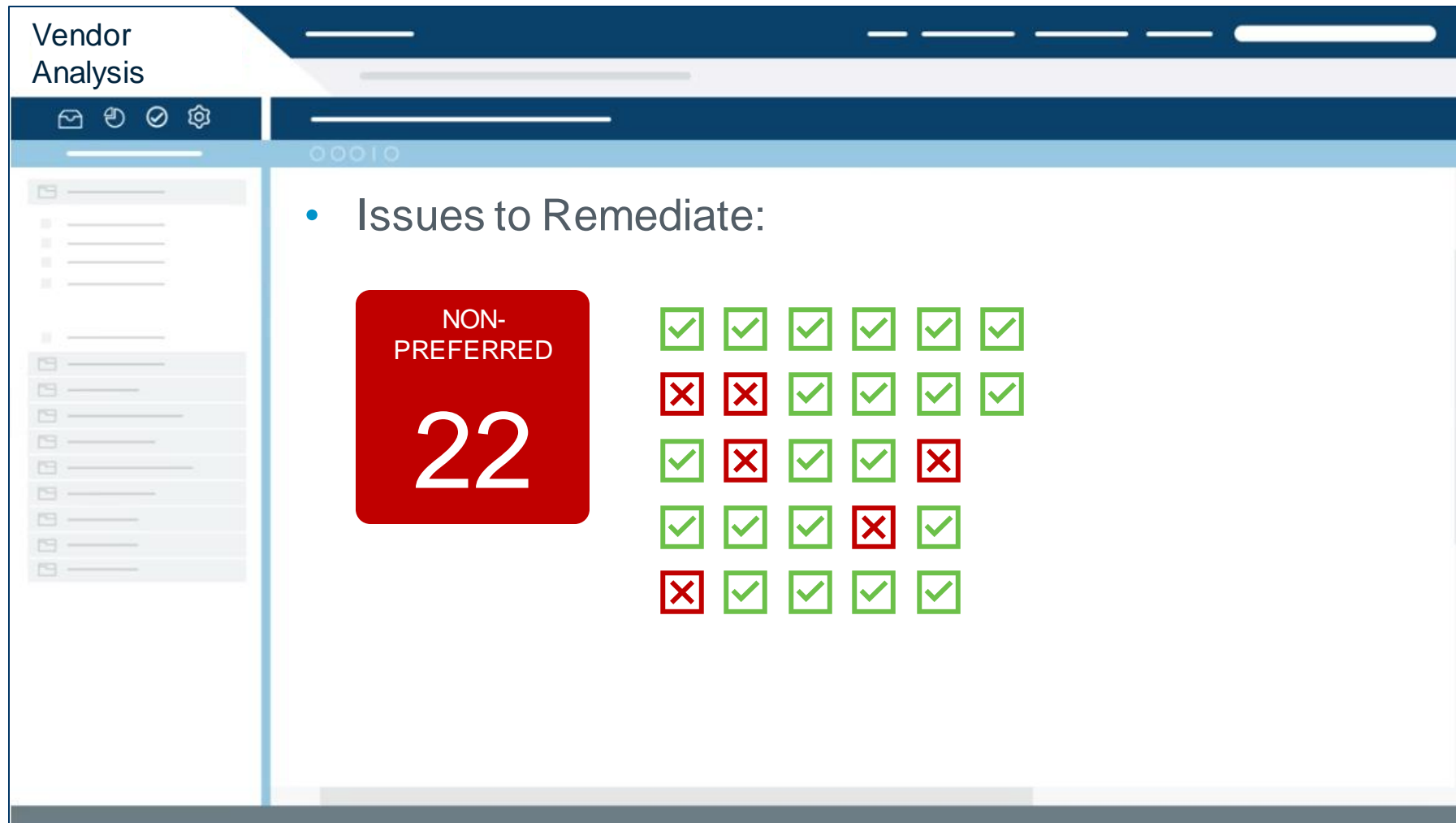


Design question sets with preferred responses that point analysts directly to potential problems.

Next-Level: Automatically generate tickets for issues identified via non-preferred responses.

Next-Level: Preferred Assessment Responses

QUICKLY IDENTIFY PROBLEM AREAS THAT REQUIRE ADDITIONAL SCRUTINY



Design question sets with preferred responses that point analysts directly to potential problems.

Next-Level: Automatically generate tickets for issues identified via non-preferred responses.

THIRD-PARTY RISK MANAGEMENT

Review & Next Steps

Ongoing Monitoring Done Right

BETTER RESULTS WITH THE SAME RESOURCES, MAXIMIZE RISK REDUCTION



Move to a proactive approach for understanding risk



Identify issues early = more time for remediation / coordination with offenders



Remediate based on pre-planned responses, improving outcomes



Independently verify vendor responses



Generate ROI via service reviews and SLA monitoring



Screen more vendors, more effectively and efficiently



Build better relationships with vendors and internal LOBs



Get a real-time view into the current state of third-party risk



Make more-informed decisions



Keep risk out of your organization

Mature Your Program Over Time

Mature Your Program Over Time



Determine
ownership and
responsibilities

Build monitoring
processes and
schedules

Mature Your Program Over Time



Determine ownership and responsibilities

Build monitoring processes and schedules



Create “emergency use” question sets

Incorporate expert vendor intelligence into reviews

Schedule and scope using inherent risk

Mature Your Program Over Time



Determine ownership and responsibilities

Build monitoring processes and schedules



Create “emergency use” question sets

Incorporate expert vendor intelligence into reviews

Schedule and scope using inherent risk



Implement fatigue-reducing capabilities for vendors

Involve lines-of-business in vendor reviews – renewal requests, service reviews, SLAs, etc.

Generate and score versus preferred responses

For More Information

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

www.processunity.com/automate

**Gartner Report Evaluates
Top Vendor Risk Tools:**

www.processunity.com/gartner

Contact ProcessUnity:

www.processunity.com/contact

Contact Ed Thomas:

ed.thomas@processunity.com

