Third Party Risk Management

Best Practices for an Effective & Efficient Program

BankBeat

ProcessUnity

Ed Thomas

Senior Vice President
ProcessUnity

PERSONAL DASHBOARD
Vendor Risk Criticality
Quarterly Assessment Schedule
Vendor Assessment Status
Contract Exposure by Service Type
Vendor Assessment Schedule
Risk Scores by Domain
Incidents Over Time by Type

Third-Party Risk Management SIMPLIFIED

Third-Party Risk Management Automation:

- Onboarding
- Due Diligence
- Ongoing Monitoring
- On-Site Control Assessments
- Performance Management
- Contract Reviews
- Service-Level Agreements
- Issue Management

2003
Founded

HQ
Concord, MA

99.9%
System Uptime
10+ Years

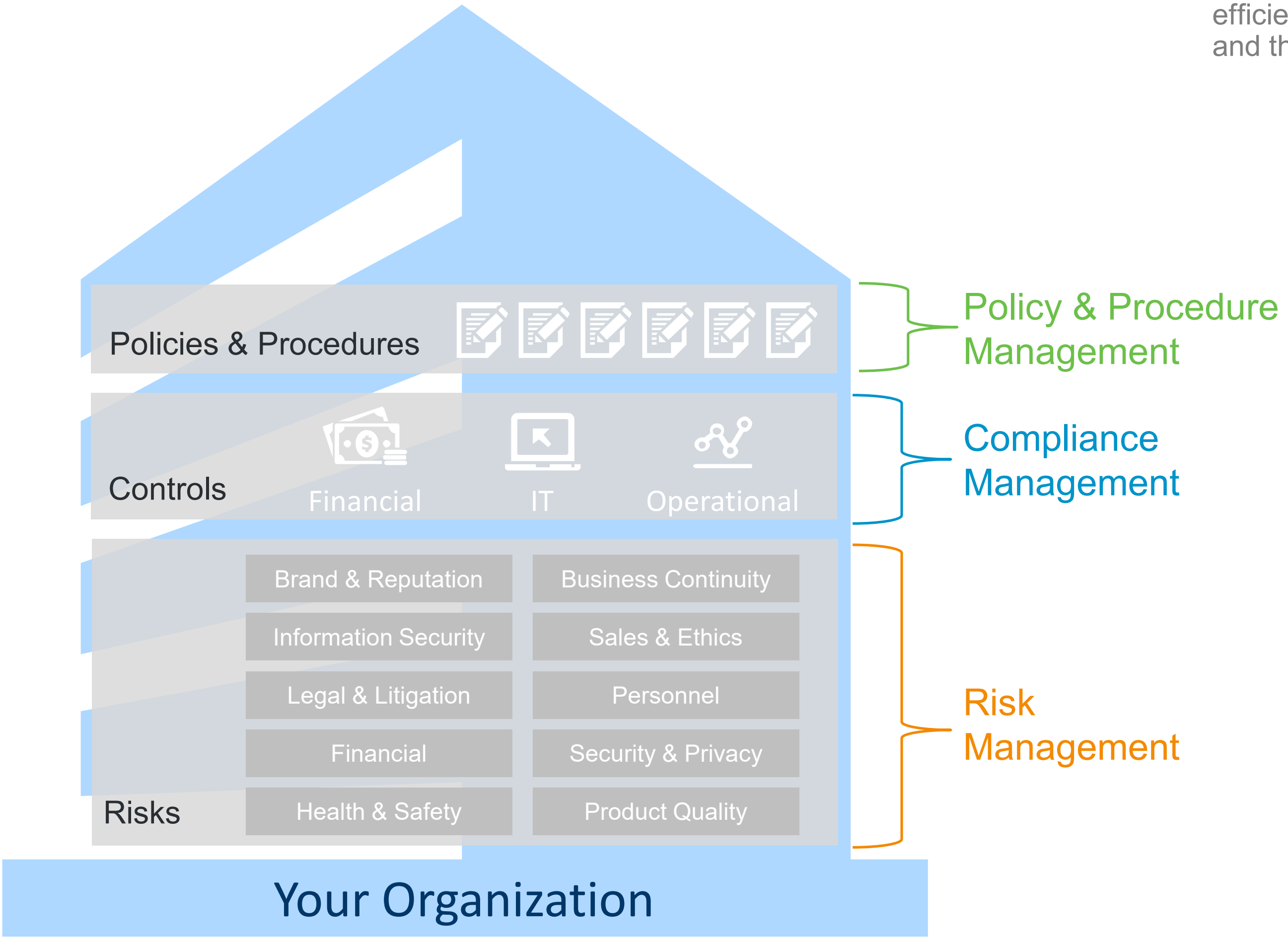
94.8%
Customer
Retention Rate

Today’s Agenda

- TPRM: Getting Grounded
- Program Building Blocks: Onboarding & Ongoing Monitoring
- Inherent Risk Best Practices
- Residual Risk & Review Cadences
- Getting Outside Help: External Content & Managed Services
- Assessing Your Program’s Maturity & Identifying Steps to Improve

TPRM: Getting Grounded

Third-Party Risk Management



Policy & Procedure Management software allows companies to more efficiently manage operations by creating a systemic approach for making decisions and the methods to deploy them in day-to-day operations

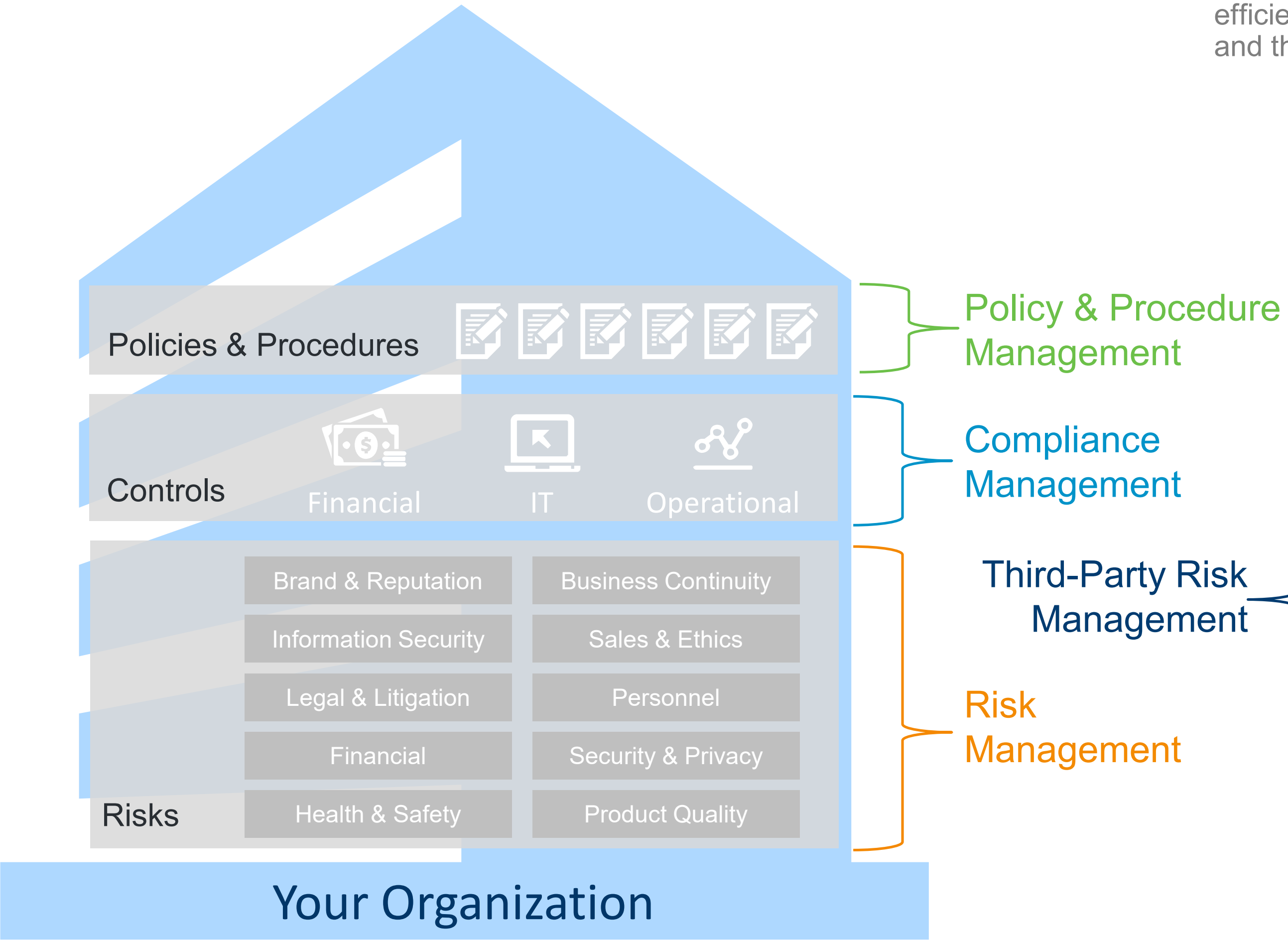
Compliance Management systems ensure that organizations are following a given set of rules and regulations and are well equipped to handle any regulatory changes

Risk Management solutions are technologies that enable a comprehensive, program that manages all aspects of risk in an organization's process

Third-Party Risk Management

Policy & Procedure Management software allows companies to more efficiently manage operations by creating a systemic approach for making decisions and the methods to deploy them in day-to-day operations

Compliance Management systems ensure that organizations are following a given set of rules and regulations and are well equipped to handle any regulatory changes



Policies & Procedures

Controls

Financial

IT

Operational

Brand & Reputation

Business Continuity

Information Security

Sales & Ethics

Legal & Litigation

Personnel

Financial

Security & Privacy

Risks

Health & Safety

Product Quality

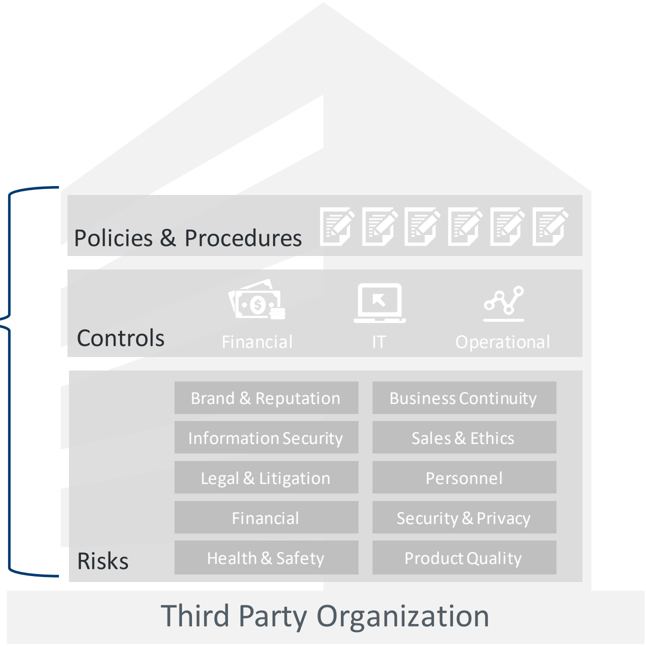
Your Organization

Policy & Procedure Management

Compliance Management

Third-Party Risk Management

Risk Management



Policies & Procedures

Controls

Financial

IT

Operational

Brand & Reputation

Business Continuity

Information Security

Sales & Ethics

Legal & Litigation

Personnel

Financial

Security & Privacy

Risks

Health & Safety

Product Quality

Third Party Organization

Third Party Risk Management solutions are applications that identify and remediate risks posed by third-party service providers

Risk Management solutions are technologies that enable a comprehensive, program that manages all aspects of risk in an organization's process

“

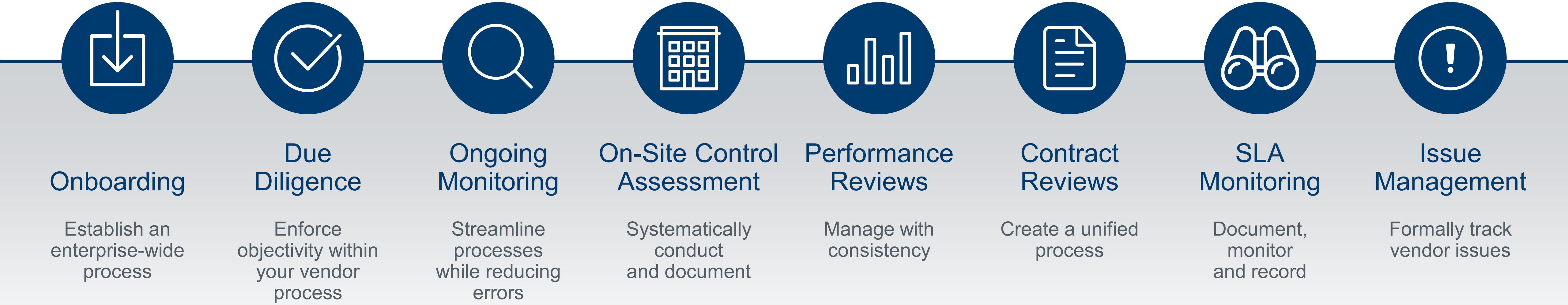
People don’t do what you ***expect*** *but what you* ***inspect****.*

- Louis V. Gerstner Jr.

”

ProcessUnity

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

The Third-Party Risk Lifecycle

How Can You Assess More Vendors, More Thoroughly… in Less Time…

Onboarding

1

Establish an enterprise-wide process

Due Diligence

2

Enforce objectivity within your vendor process

Ongoing Monitoring

3

Streamline processes while reducing errors

The Third-Party Risk Lifecycle

…So Your Team Can Spend More Time Reducing Risk and Generating ROI.

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

A Few of the Challenges Organizations Face Today

Identifying / Grouping Critical Vendor by Risk Tier

- Who are our critical outsourced third-parties?
- What services are they providing?
- Where are they located?
- How do we risk-tier our vendor database?

Establishing a Framework / Process for Internal & External Review

- How do we ensure adoption and compliance across the organization?
- How can we improve vendor responsiveness / reduce fatigue?
- How do we improve executive support / communication?

Storing Supporting Documentation

- How and when do we reassess third parties?
- How do we organize the data from our vendor population?

Determining Which Fourth (Fifth?) Parties to Assess

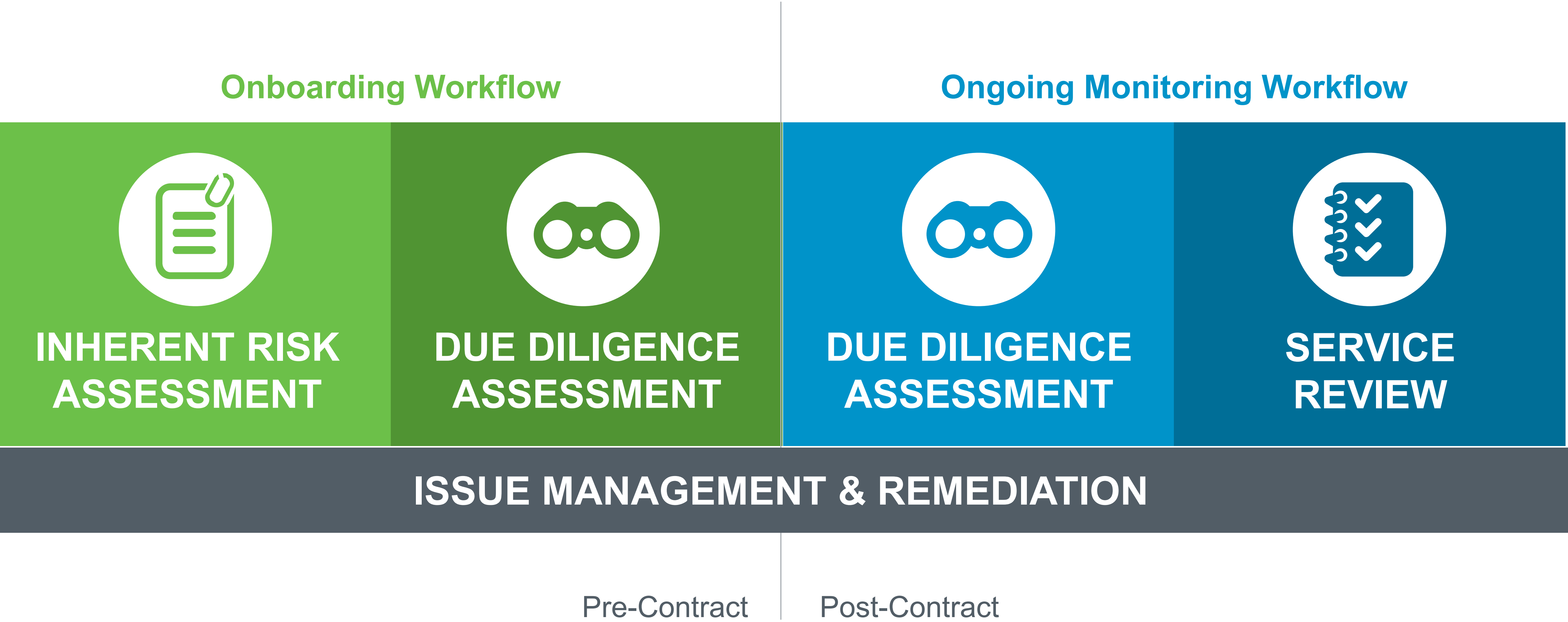
- Which vendors are using fourth parties to deliver services?
- How far down the chain do we have to go to feel secure?

It’s Not Going to Get Easier

- More third-parties (and fourth-parties)
- More / new / different threats
- Evolving regulations (EBA, GDPR, CCPA, FCA, PCI, HIPAA, DPA)
- Vendors are buckling under the load

Program Building Blocks

Building Blocks: Base Processes & Flows



Onboarding Workflow

INHERENT RISK ASSESSMENT

DUE DILIGENCE ASSESSMENT

Ongoing Monitoring Workflow

DUE DILIGENCE ASSESSMENT

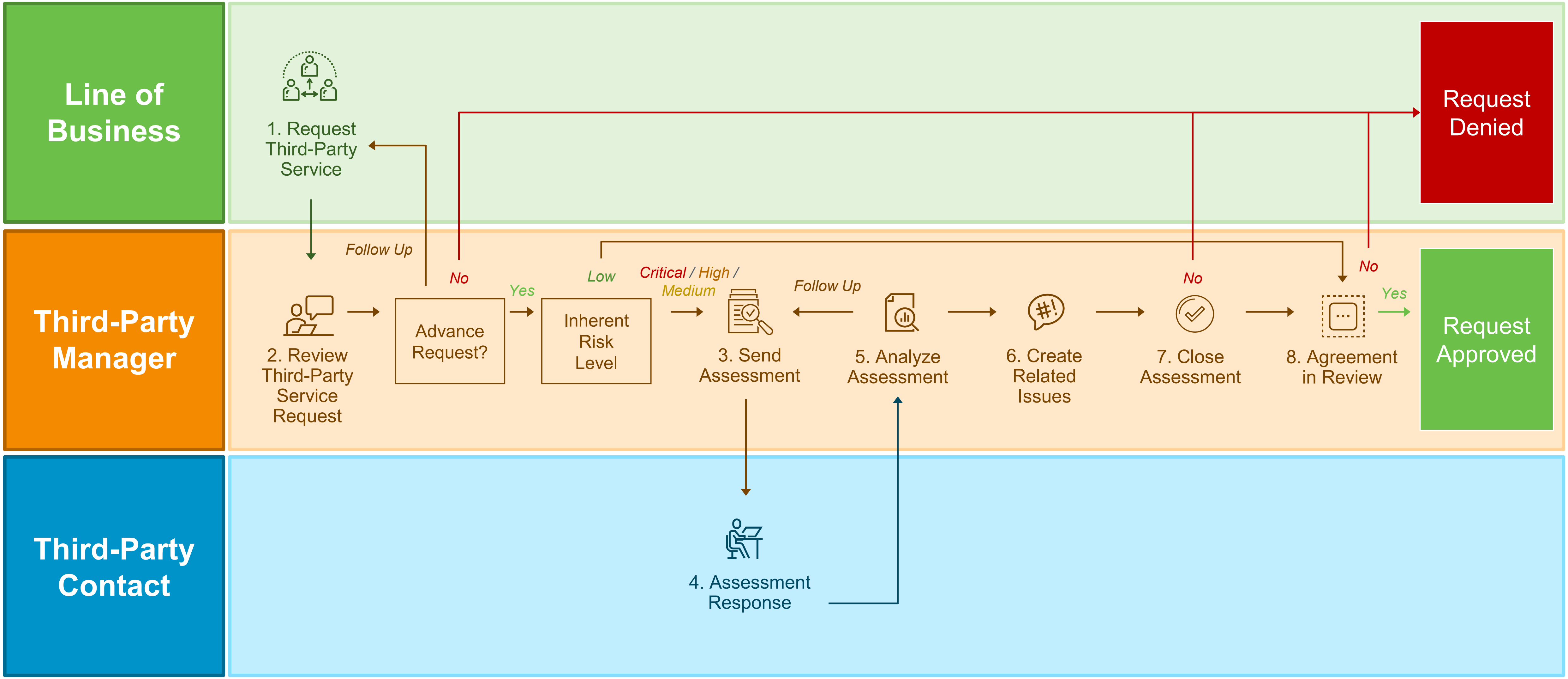
SERVICE REVIEW

ISSUE MANAGEMENT & REMEDIATION

Pre-Contract

Post-Contract

Onboarding Workflow



Line of Business

Third-Party Manager

Third-Party Contact

1. Request Third-Party Service

2. Review Third-Party Service Request

Follow Up

Advance Request?

No

Yes

Inherent Risk Level

Low

Critical / High / Medium

3. Send Assessment

4. Assessment Response

Follow Up

5. Analyze Assessment

6. Create Related Issues

7. Close Assessment

No

8. Agreement in Review

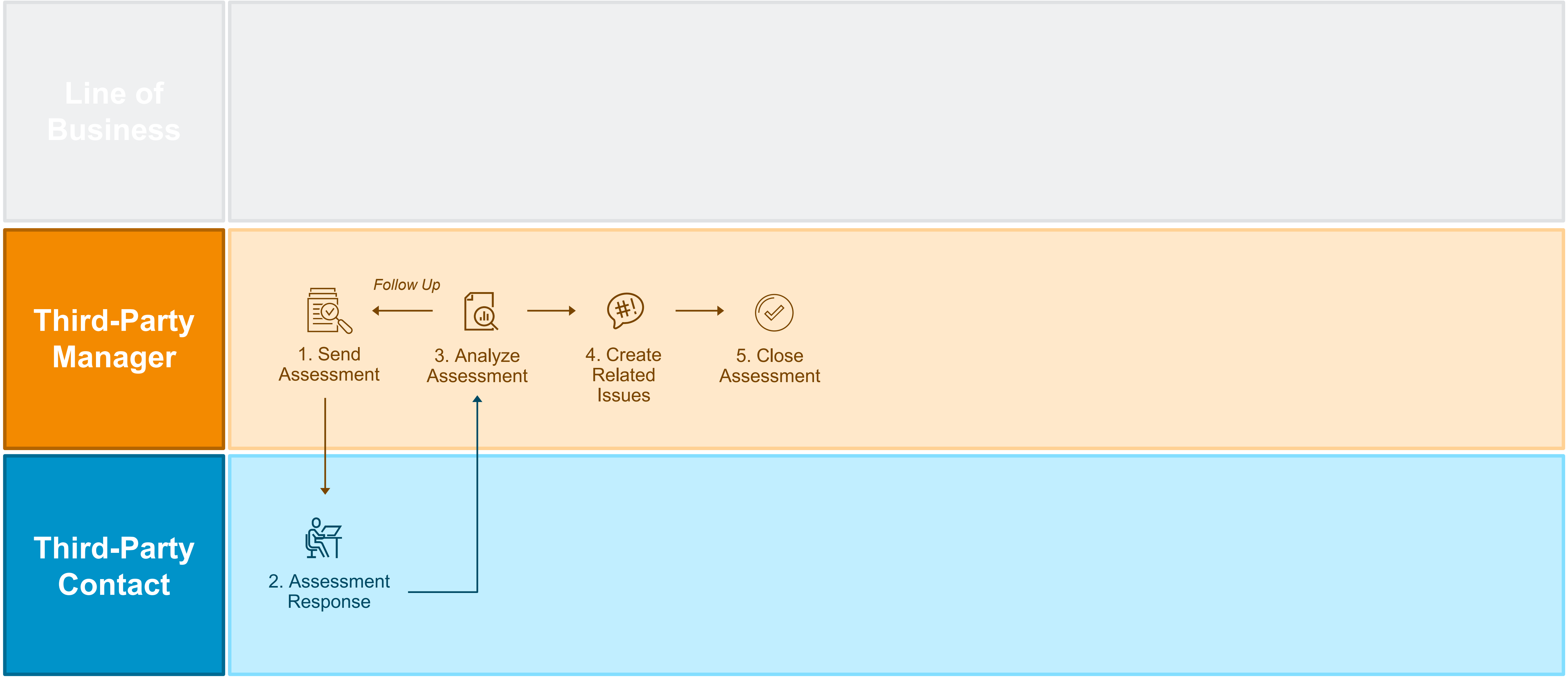
No

Yes

Request Denied

Request Approved

Ongoing Monitoring: Periodic Due Diligence



Line of Business

Third-Party Manager

1. Send Assessment

Follow Up

3. Analyze Assessment

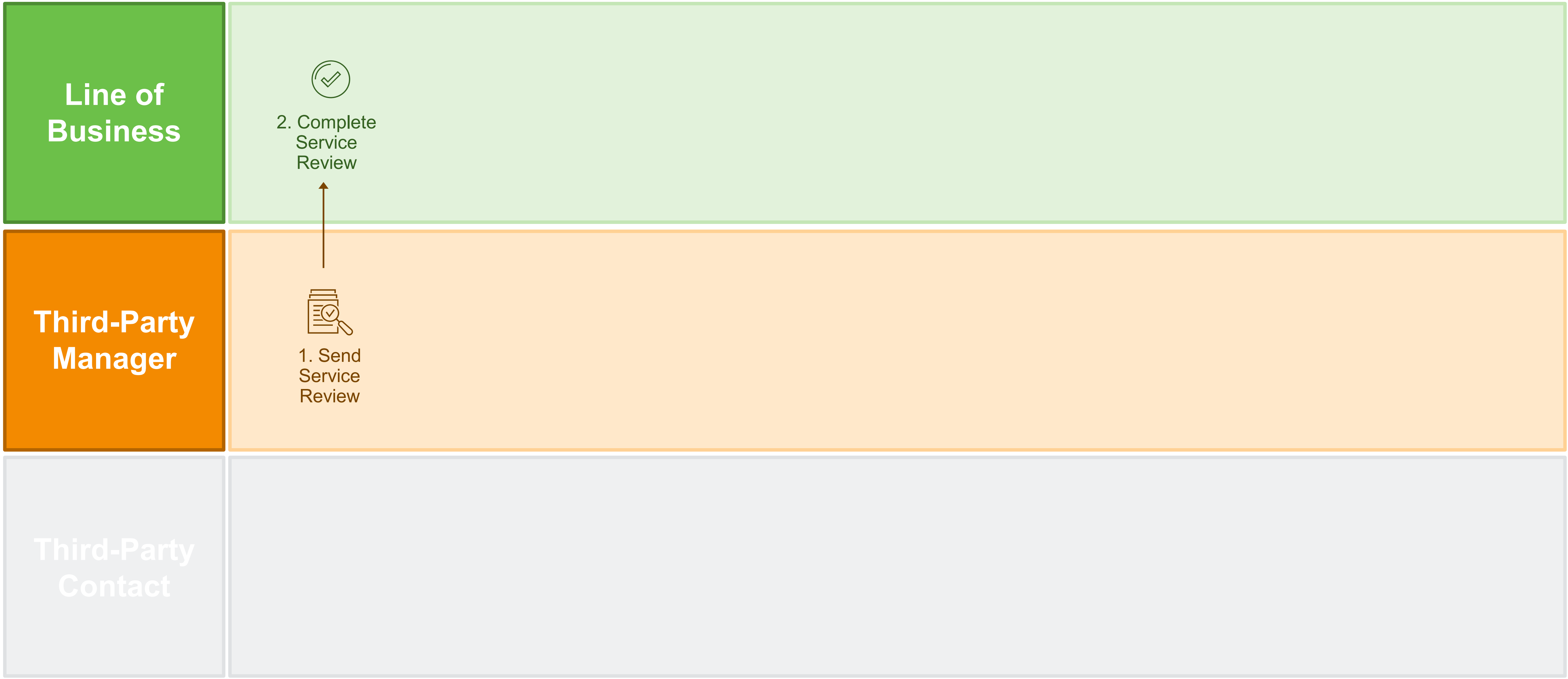
4. Create Related Issues

5. Close Assessment

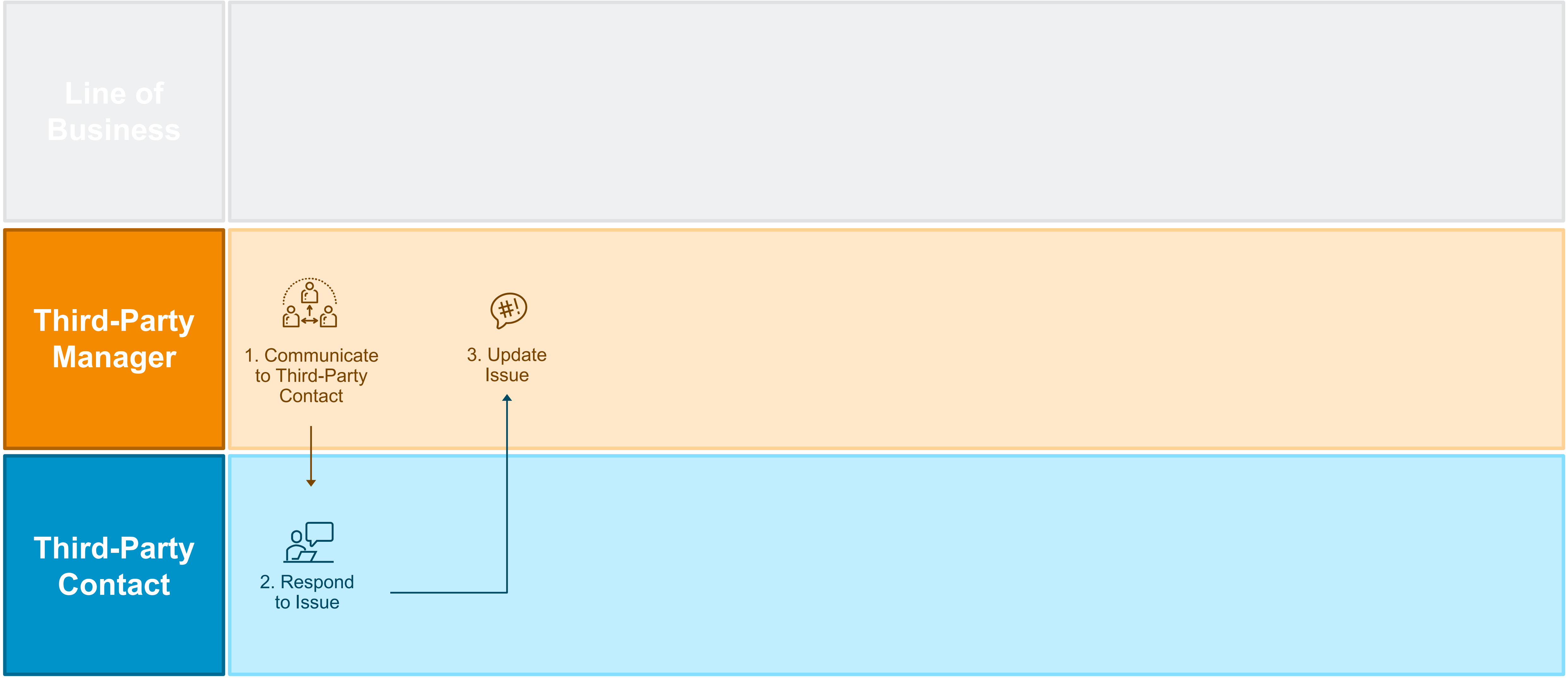
Third-Party Contact

2. Assessment Response

Ongoing Monitoring: Service Reviews



Issue Management & Remediation



Line of Business

Third-Party Manager

1. Communicate to Third-Party Contact

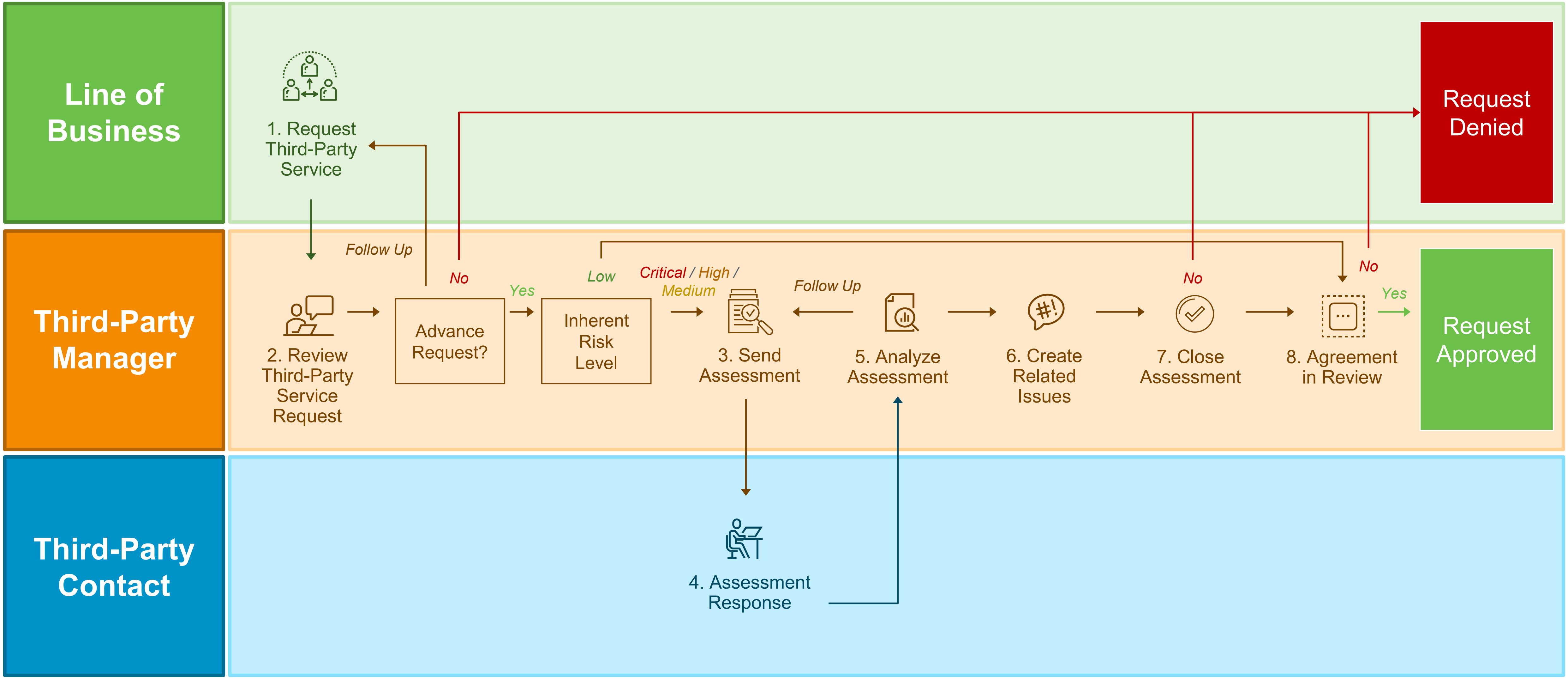
3. Update Issue

Third-Party Contact

2. Respond to Issue

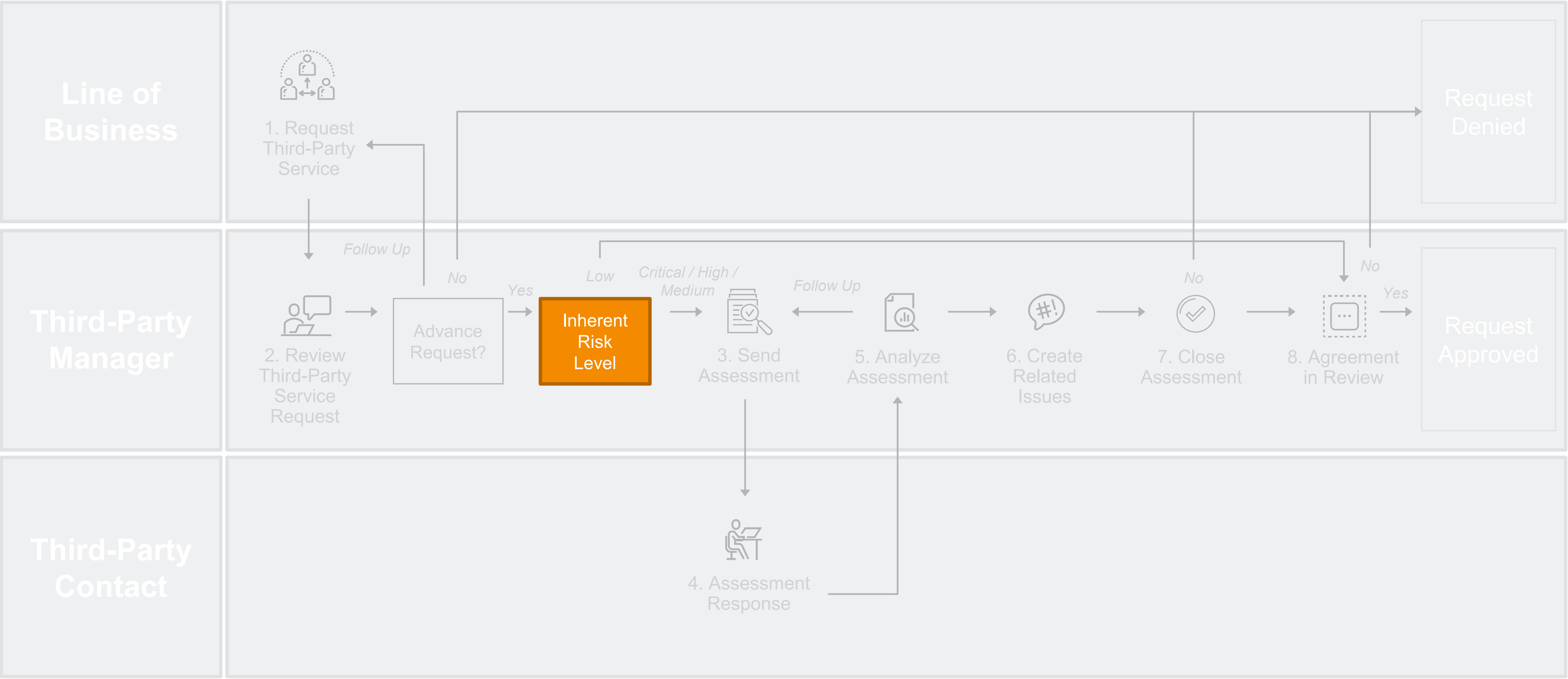
Inherent Risk

Onboarding Workflow



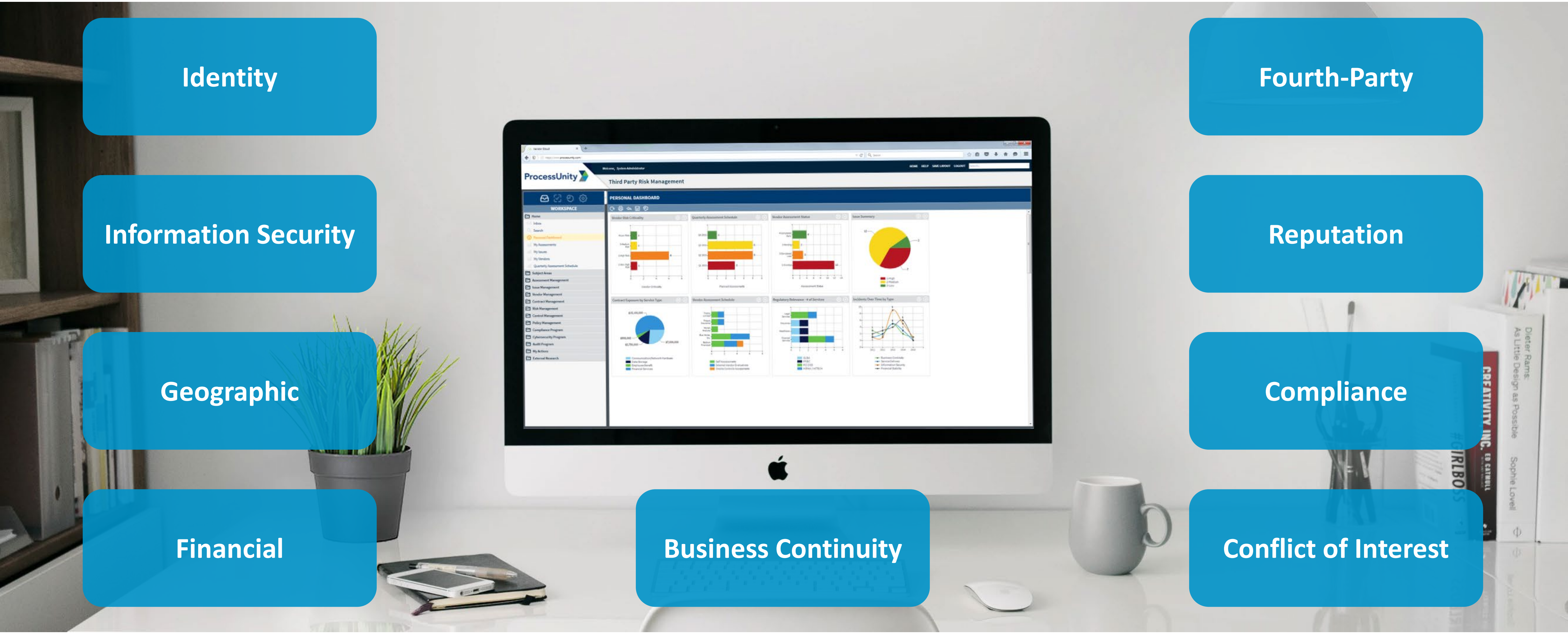
ProcessUnity

Onboarding Workflow



ProcessUnity

Risk Domains Help Define Inherent Risk Questions



Identity

Information Security

Geographic

Financial

Business Continuity

Fourth-Party

Reputation

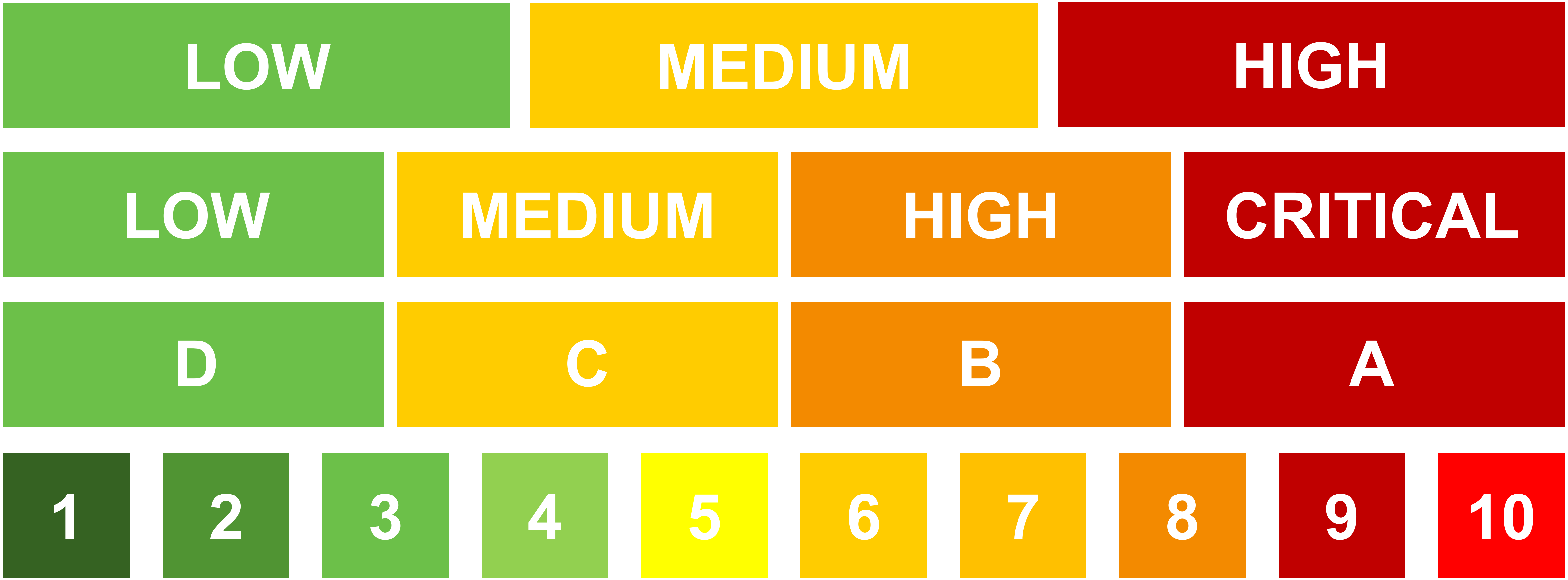
Compliance

Conflict of Interest

Define Your Inherent Risk Questions

- What is the expected annual contract amount? (Financial / Business Continuity)
- Is the third-party service performed domestically? (Geographic)
- Is the service essential to the operations of the company? (Business Continuity)
- How difficult would it be to replace this service with an alternative? (Business Continuity)
- What is the expected annual volume of records that will be accessed, processed, stored or transmitted by this third party? (Information Security)
- Is any part of the third-party service being provided subject to any regulatory / compliance requirements? (Compliance)
- Does this third-party store, process or transmit Personally Identifiable Information (PII) or Protected Health Information (PHI) as part of this service? (Information Security)
- Is the service delivered as a cloud-based solution? (Information Security)
- Does this third party have access to our IT network or technical infrastructure? (Information Security)
- Does the third party outsource any part of the service? (Geographic / Information Security)

Define Your Risk Tiers



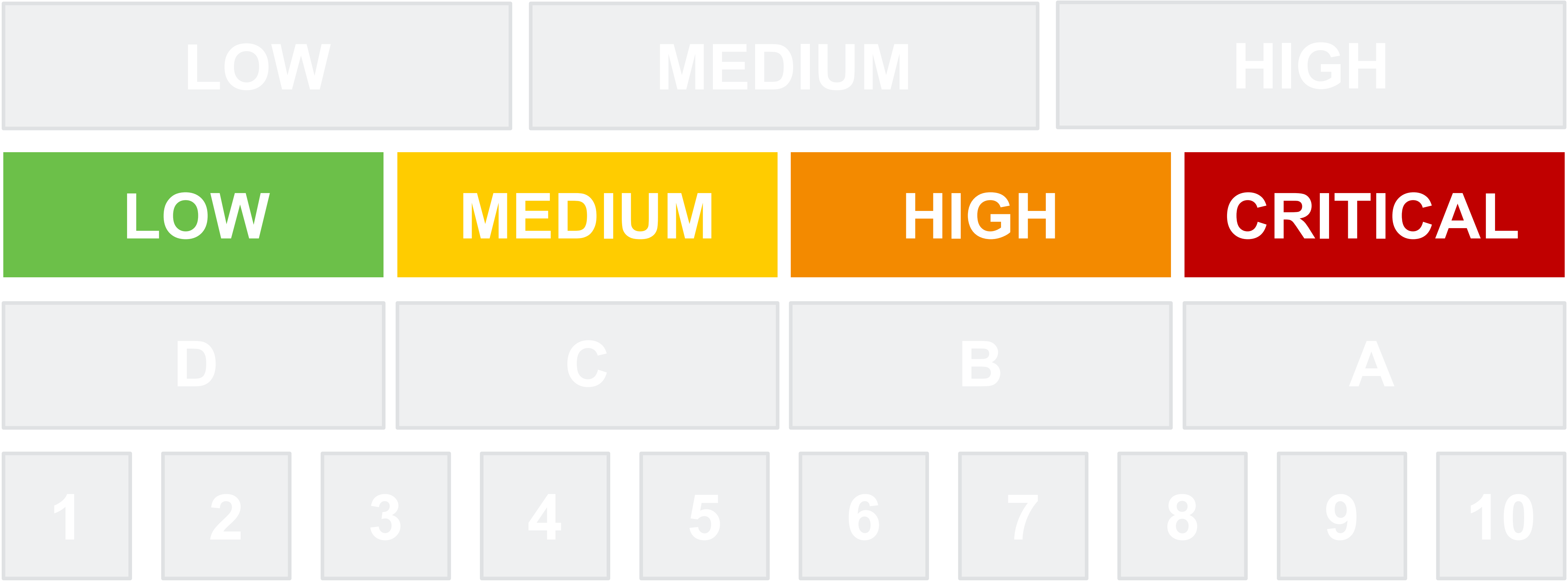
LOW | MEDIUM | HIGH

LOW | MEDIUM | HIGH | CRITICAL

D | C | B | A

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Define Your Risk Tiers



LOW | MEDIUM | HIGH

LOW | MEDIUM | HIGH | CRITICAL

D | C | B | A

1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

Building a Scoring System

- What is the expected annual contract amount? (Financial / Business Continuity)
- Is the third-party service performed domestically? (Geographic)
- Is the service essential to the operations of the company? (Business Continuity)
- How difficult would it be to replace this service with an alternative? (Business Continuity)
- What is the expected annual volume of records that will be accessed, processed, stored or transmitted by this third party? (Information Security)
- Is any part of the third-party service being provided subject to any regulatory / compliance requirements? (Compliance)
- Does this third-party store, process or transmit Personally Identifiable Information (PII) or Protected Health Information (PHI) as part of this service? (Information Security)
- Is the service delivered as a cloud-based solution? (Information Security)
- Does this third party have access to our IT network or technical infrastructure? (Information Security)
- Does the third party outsource any part of the service? (Geographic / Information Security)

Building a Scoring System

Is the service essential to the operations of the company? **YES** = **CRITICAL**

Building a Scoring System

How difficult would it be to replace this service with an alternative?

Is any part of the third-party service being provided subject to any regulatory / compliance requirements?

Does this third-party store, process or transmit PII or PHI as part of this service?

Is the service delivered as a cloud-based solution?

Does this third party have access to our IT network or technical infrastructure?

+ Does the third party outsource any part of the service?

= **CRITICAL**

Building a Scoring System

How difficult would it be to replace this service with an alternative?

Is any part of the third-party service being provided subject to any regulatory / compliance requirements?

Does this third-party store, process or transmit PII or PHI as part of this service?

Is the service delivered as a cloud-based solution?

Does this third party have access to our IT network or technical infrastructure?

+ Does the third party outsource any part of the service?

= Is the service essential to the operations of the company?

Building a Scoring System

How difficult would it be to replace this service with an alternative? 2 Points

Is any part of the third-party service being provided subject to any regulatory / compliance requirements? 2 Points

Does this third-party store, process or transmit PII or PHI as part of this service? 2 Points

Is the service delivered as a cloud-based solution? 2 Points

Does this third party have access to our IT network or technical infrastructure? 2 Points

+ Does the third party outsource any part of the service? 2 Points

= Is the service essential to the operations of the company? 12 Points

Building a Scoring System

LOW	MEDIUM	HIGH	CRITICAL
0 - 5	*6 - 7*	*8 - 11*	*12 +*

Intake Questions & Point Values

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

ProcessUnity

Checking the Math

	MAJOR BANK	RECORDS SHREDDER	LANDSCAPING CONTRACTOR
Essential to operations	YES (12 Points)	NO	NO
Contract > $500,000		NO	NO
Performed internationally		NO	NO
Difficult to replace		YES (2 Points)	NO
High record volume		YES (2 Points)	NO
Subject to regulatory requirements		YES (2 Points)	NO
Access to PII or PHI		YES (2 Points)	NO
Cloud-based solution		NO	NO
Access to technical infrastructure		NO	NO
Outsources a portion of the service		NO	YES (2 Points)
TOTAL SCORE	12	8	2
RISK TIER	CRITICAL	HIGH	LOW

Use Inherent Risk to Auto Scope Due Diligence

LOW *0 - 5*	MEDIUM *6 - 7*	HIGH *8 - 11*	CRITICAL *12 +*
No Further Due Diligence Required	Light Due Diligence Required (SIG Lite)	Medium Due Diligence Required (SIG Lite)	Intensive Due Diligence Required (SIG Core)

Quick Sidebar: Questionnaires

The Evolution of the Assessment Questionnaire

One, (usually long) questionnaire used to assess all vendors

ONE SIZE “FITS” ALL

Multiple questionnaires of varying lengths used to vet vendors in different risk tiers

MULTIPLE VERSIONS

A single, smart assessment that includes questions based on inherent risk and adjusts mid-assessment based on vendors’ answers

SELF-SCOPING

Smart assessment that pre-scores answers (good vs bad) and automatically generates issues and follow-ups to reduce review time

SELF-SCORING

Inherent Risk Scoring

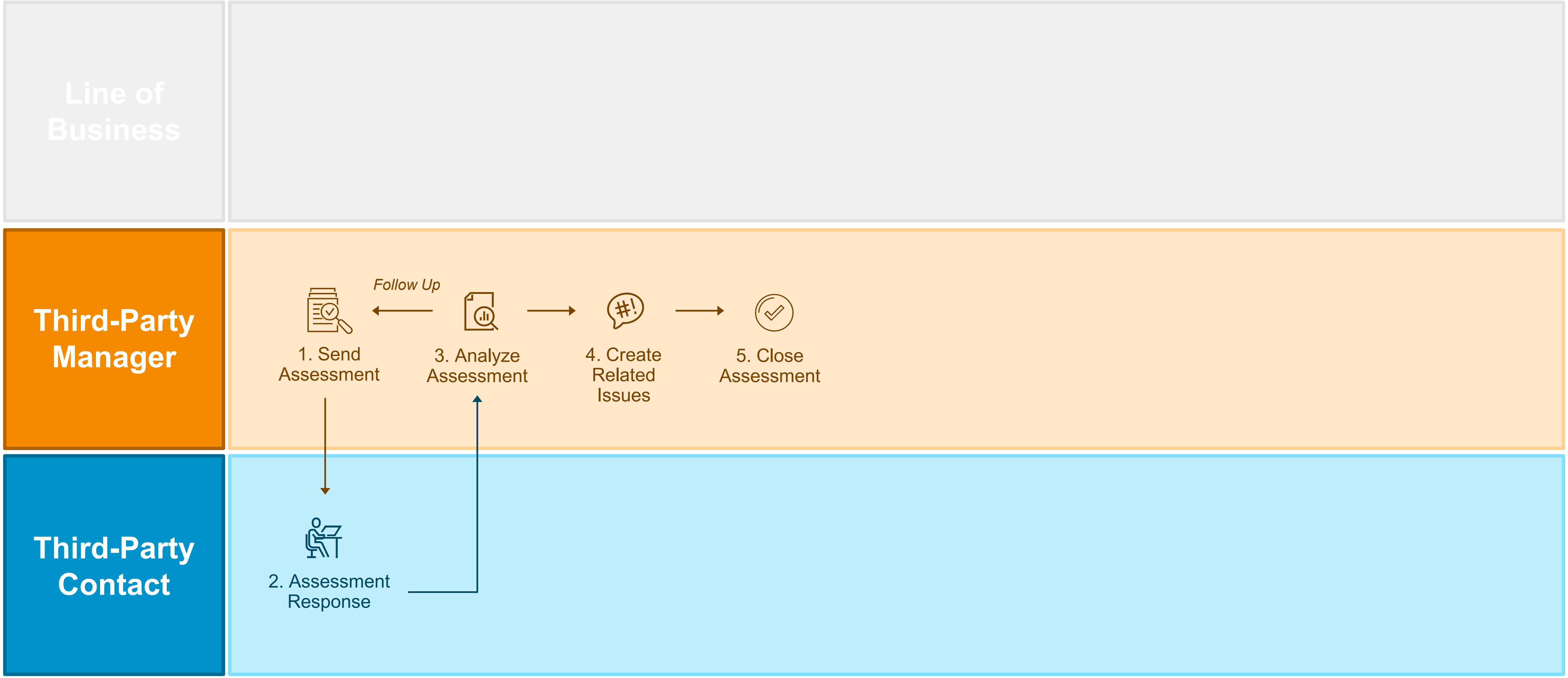
LOW	MEDIUM	HIGH	CRITICAL
0 - 5	*6 - 7*	*8 - 11*	*12 +*

Intake Questions & Point Values

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

Determining a Cadence for Periodic Due Diligence

Ongoing Monitoring: Periodic Due Diligence



ProcessUnity

Residual Risk Determines Scope & Frequency

Inherent Risk		Previous Assessment Review Rating		Residual Risk	Assessment Scope	Assessment Frequency
CRITICAL	+	No Prior Review	=	Critical	SIG Core	ASAP
		Unsatisfactory		Critical	SIG Core	Annual
		Needs Improvement		Critical	SIG Core	Annual
		Satisfactory		High	SIG Lite	Annual
HIGH	+	No Prior Review	=	High	SIG Lite	ASAP
		Unsatisfactory		High	SIG Lite	Biennial
		Needs Improvement		High	SIG Lite	Biennial
		Satisfactory		Medium	SIG Lite	Biennial
MEDIUM	+	No Prior Review	=	Medium	SIG Lite	ASAP
		Unsatisfactory		Medium	SIG Lite	Biennial
		Needs Improvement		Medium	SIG Lite	Biennial
		Satisfactory		Low	SIG Lite	Triennial
LOW	+	N/A	=	Low	N/A	N/A
		N/A		Low	N/A	N/A
		N/A		Low	N/A	N/A
		N/A		Low	N/A	N/A

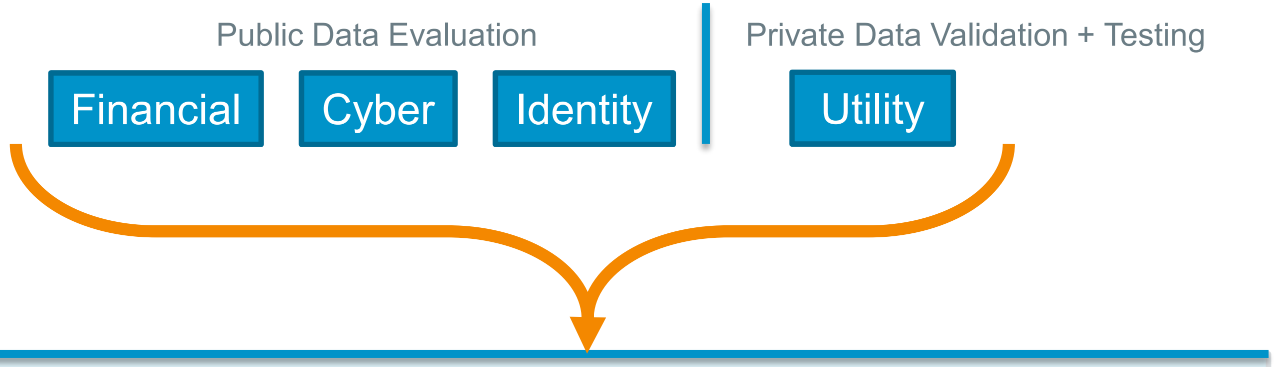
ProcessUnity

Get Help: External Content & Managed Services

Incorporate External Ratings & Content

Enriched Content Options

- Understand the difference between public and private data validation
- Set a rationale for leveraging by inherent risk tier
- Off-load the time intense operations
- Embed external content into your process



Public Data Evaluation

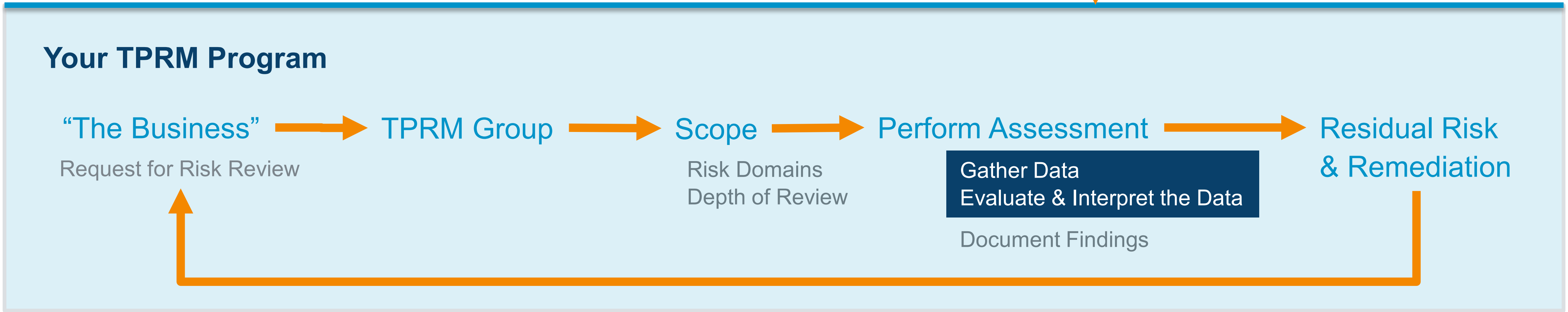
Financial

Cyber

Identity

Private Data Validation + Testing

Utility



Your TPRM Program

“The Business” → TPRM Group → Scope → Perform Assessment → Residual Risk & Remediation

Request for Risk Review

Risk Domains
Depth of Review

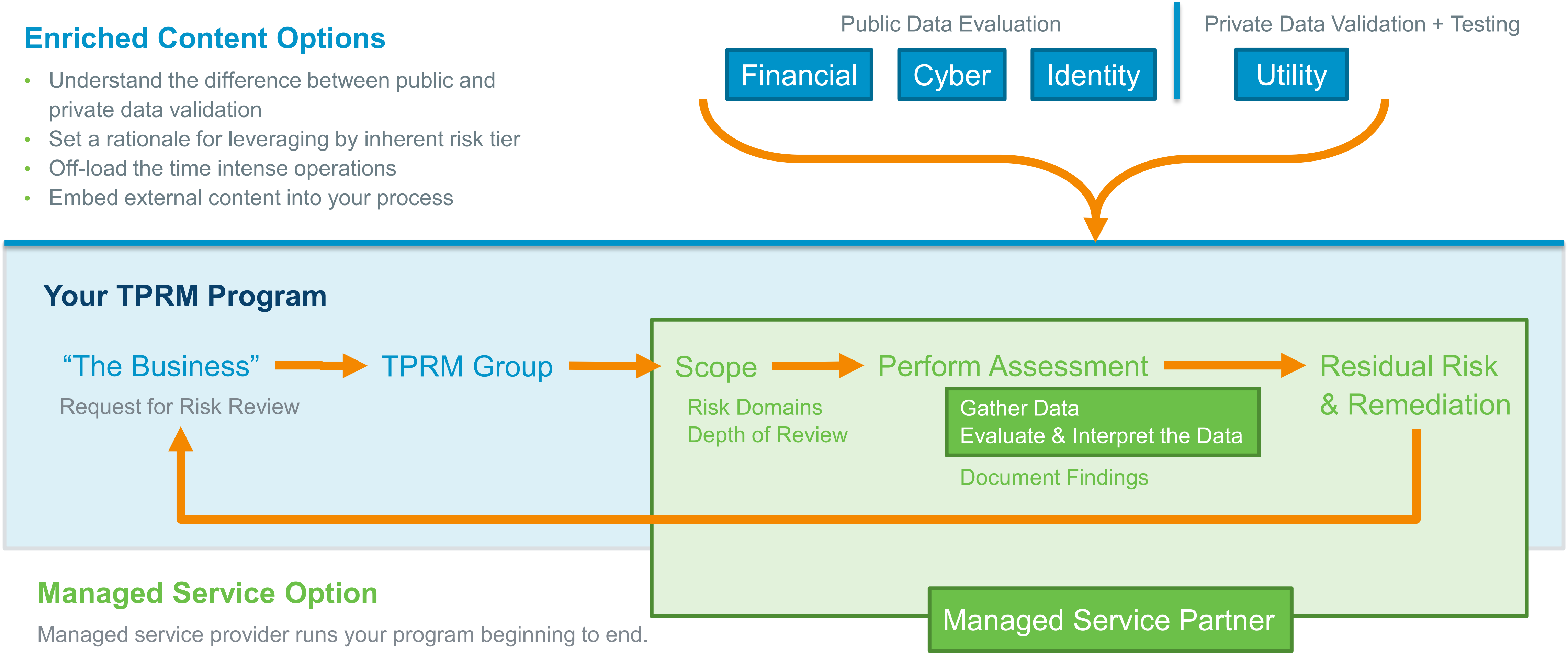
Gather Data
Evaluate & Interpret the Data

Document Findings

Extend Your Team

Enriched Content Options

- Understand the difference between public and private data validation
- Set a rationale for leveraging by inherent risk tier
- Off-load the time intense operations
- Embed external content into your process



Managed Service Option

Managed service provider runs your program beginning to end.

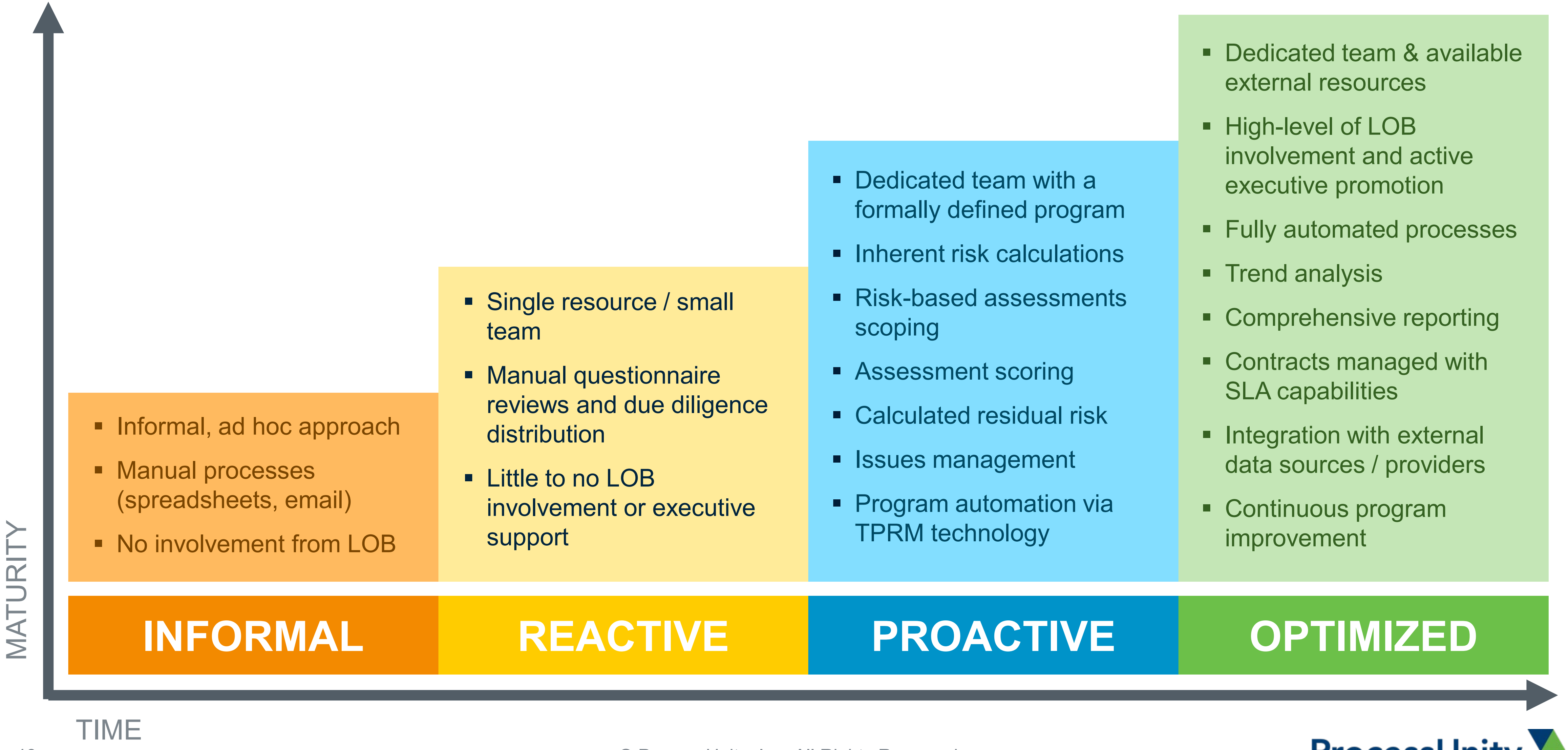
- You adopt or dictate the risk methodology
- You confirm/accept the risk
- You monitor and leverage the process

Getting Help is Great, But Always Remember…

You Own the Risk!

Assessing Your Program's Maturity

Third-Party Risk Maturity Model



INFORMAL

- Informal, ad hoc approach
- Manual processes (spreadsheets, email)
- No involvement from LOB

REACTIVE

- Single resource / small team
- Manual questionnaire reviews and due diligence distribution
- Little to no LOB involvement or executive support

PROACTIVE

- Dedicated team with a formally defined program
- Inherent risk calculations
- Risk-based assessments scoping
- Assessment scoring
- Calculated residual risk
- Issues management
- Program automation via TPRM technology

OPTIMIZED

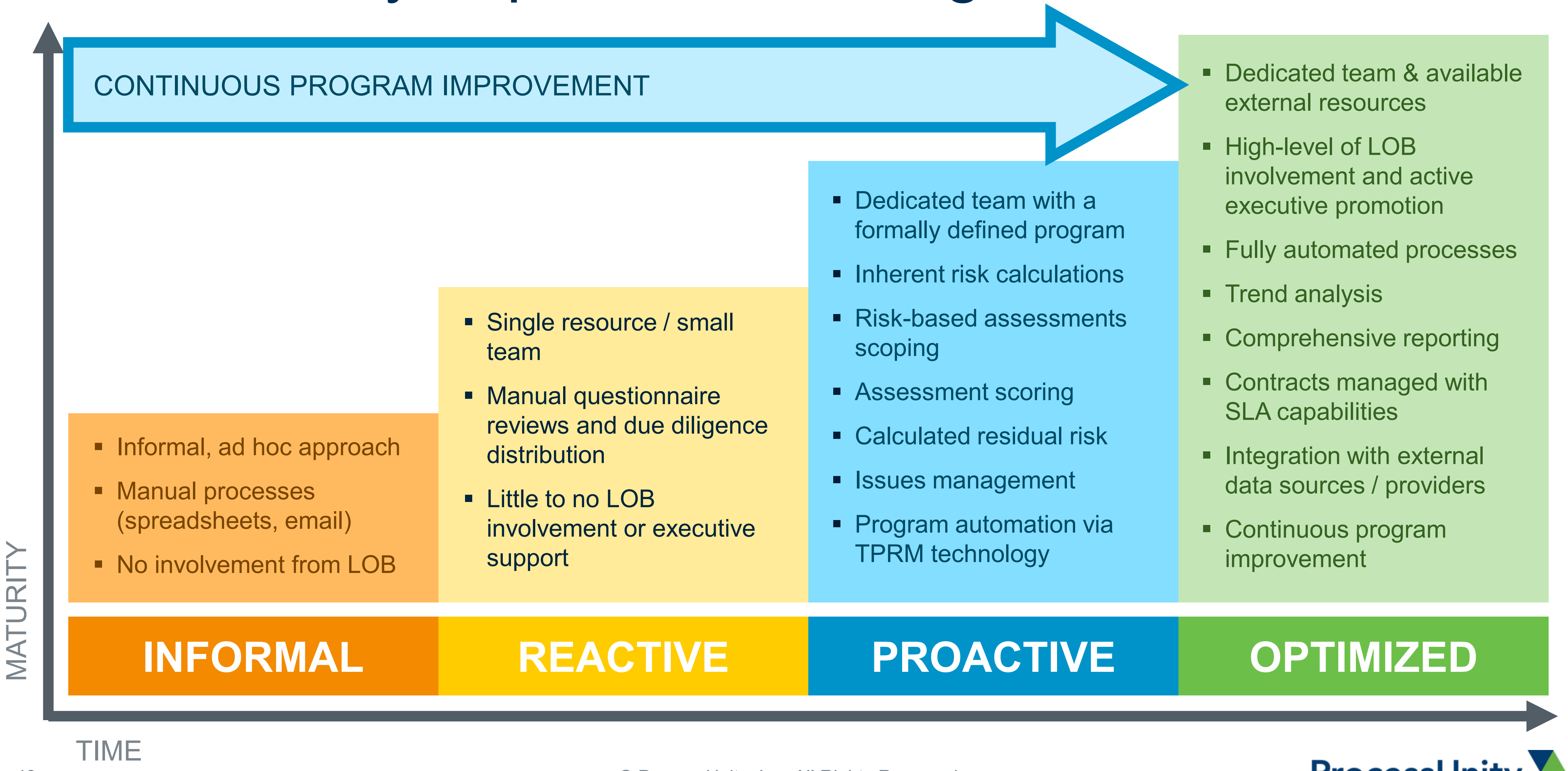
- Dedicated team & available external resources
- High-level of LOB involvement and active executive promotion
- Fully automated processes
- Trend analysis
- Comprehensive reporting
- Contracts managed with SLA capabilities
- Integration with external data sources / providers
- Continuous program improvement

POLL QUESTION:

How would you rate the maturity level of your current TPRM program?

INFORMAL	REACTIVE	PROACTIVE	OPTIMIZED

Incrementally Improve Your Program



INFORMAL

- Informal, ad hoc approach
- Manual processes (spreadsheets, email)
- No involvement from LOB

REACTIVE

- Single resource / small team
- Manual questionnaire reviews and due diligence distribution
- Little to no LOB involvement or executive support

PROACTIVE

- Dedicated team with a formally defined program
- Inherent risk calculations
- Risk-based assessments scoping
- Assessment scoring
- Calculated residual risk
- Issues management
- Program automation via TPRM technology

OPTIMIZED

- Dedicated team & available external resources
- High-level of LOB involvement and active executive promotion
- Fully automated processes
- Trend analysis
- Comprehensive reporting
- Contracts managed with SLA capabilities
- Integration with external data sources / providers
- Continuous program improvement

Incrementally Improve Your Program

Take steps to advance your program (and your career)

INFORMAL

- Formalize your program
- Document, document, document
- Socialize program’s charter with executives
- **Advantage: Blank slate**

REACTIVE

- Nix the one-size-fits all questionnaire
- Implement a repository for TPRM data
- Calculate inherent and residual risk
- Look to automation
- **Advantage: Leverage your recent experience to determine what’s working…and what’s not working**

PROACTIVE

- Increase LOB involvement and executive promotion
- Extend beyond onboarding and due diligence
- Improve contract management and SLA tracking
- Incorporate external data into onboarding and continuous monitoring
- **Advantage: Consistency builds confidence with regulators**

OPTIMIZED

- Focus on cost reduction and vendor service quality
- **Advantage: Improved negotiation power based on accurate, actionable data on vendors’ ability to meet KPIs, SLAs and other performance metrics**

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