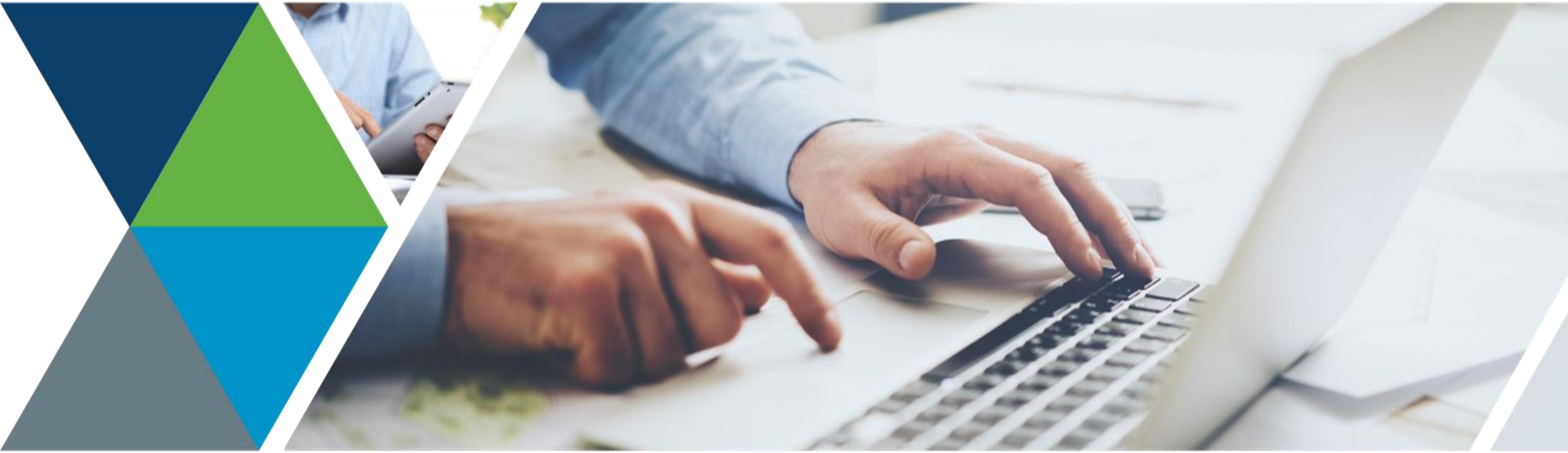
The Power Your Third-Party Risk Program Can Deliver in Challenging Times



BITSIGHT®

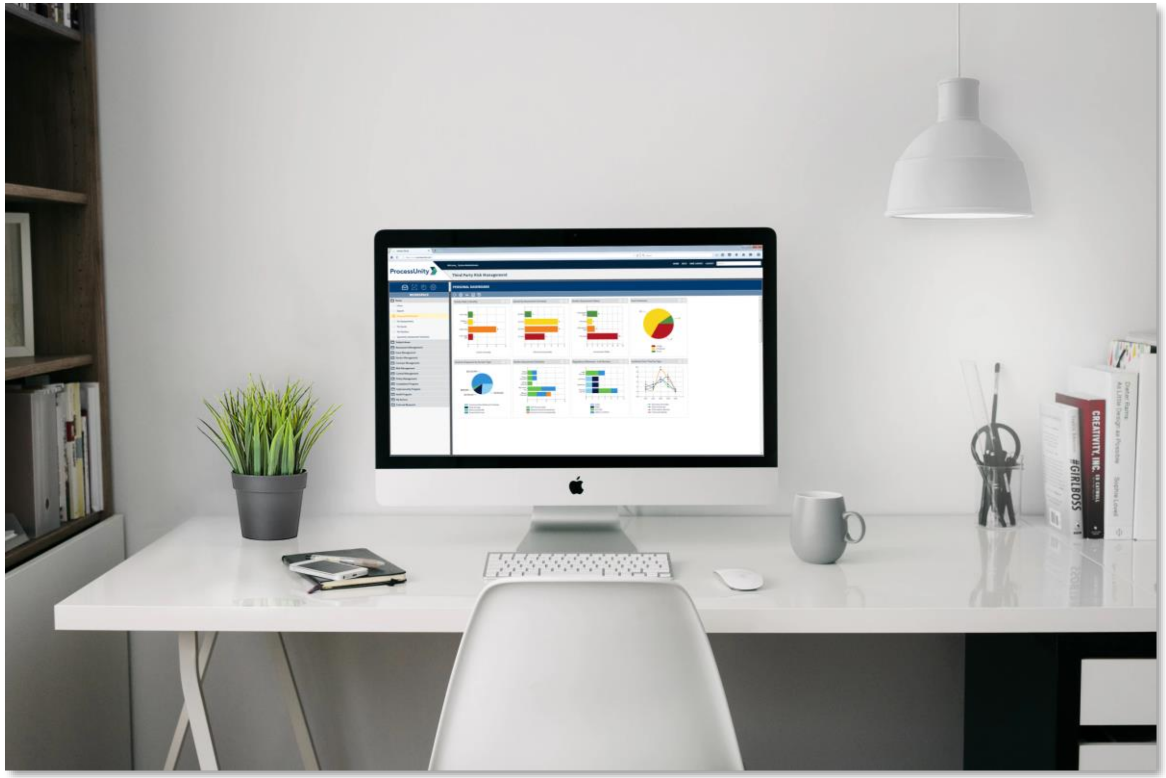
ProcessUnity

David Klein
Senior Director of Product Strategy
ProcessUnity

Leslie Sloan
Consulting Engineer
BitSight

Today’s Agenda

- Intros
- A few minutes on The Black Swan
- Getting the House in Order: Re-assessing the building blocks
- Enriching the Third-Party Risk Management Workflow
- Getting Outside Help: External Content & Managed Services



ProcessUnity

The Leader in Third-Party Risk Management Automation

- Programs for organizations of all sizes and maturity
- Built-in best practices
- Unparalleled subject matter expertise
- Short deployment times
- Hundreds of successful customer implementations

Third-Party Risk Lifecycle Support

Onboarding
Establish an enterprise-wide process

Due Diligence
Enforce objectivity within your vendor process

Ongoing Monitoring
Streamline processes while reducing errors

On-Site Control Assessments
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

Automated Scoring & Scoping
Assess vendors appropriately based on inherent & residual risk

Content Integration
Incorporate financial and cyber ratings into your due diligence

Powerful Configuration
Future-proof platform changes as your program matures

Smart Questionnaires
Reduce vendor fatigue & auto-score responses

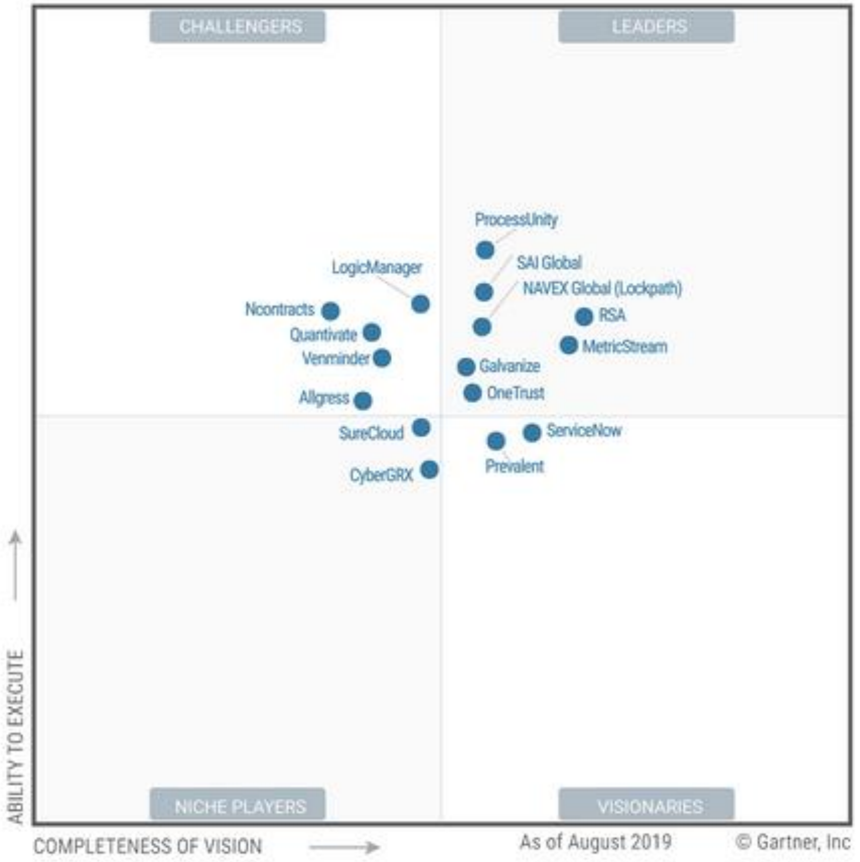
SIG Integration
Leverage SIG content in your questionnaires

Recognized by Gartner
Read the reports at **processunity.com/gartner**

ProcessUnity

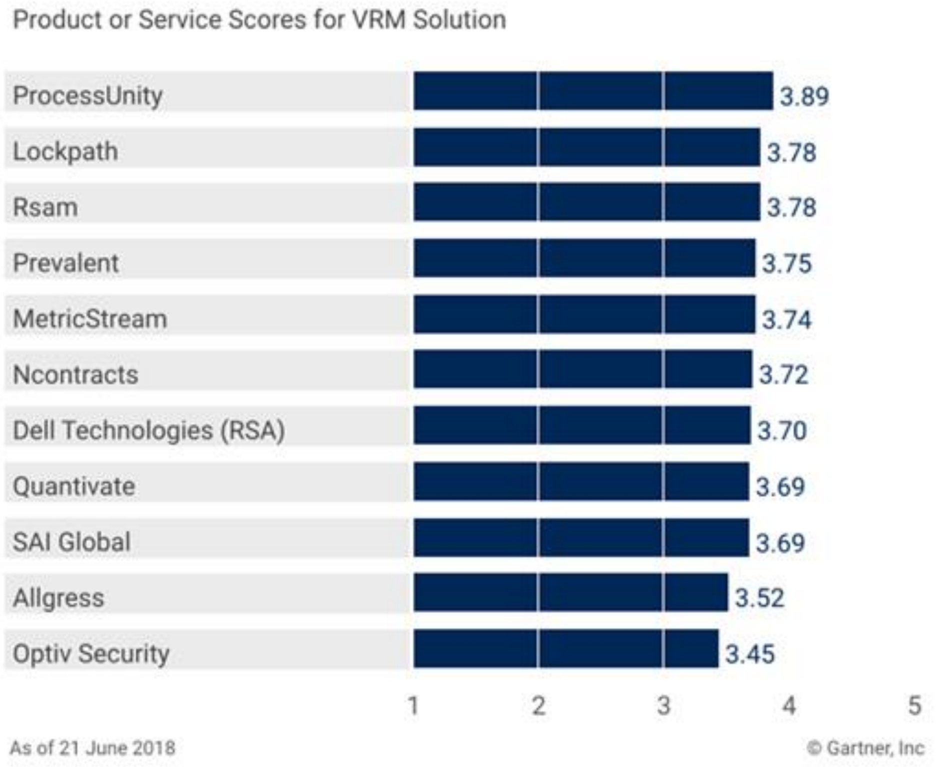
Two Gartner Reports. Two Recognitions in IT Vendor Risk Management Software.

Figure 1. Magic Quadrant for IT Vendor Risk Management Tools



Source: Gartner (November 2019)

Figure 1. Vendors' Product Scores for the VRM Solution Use Case



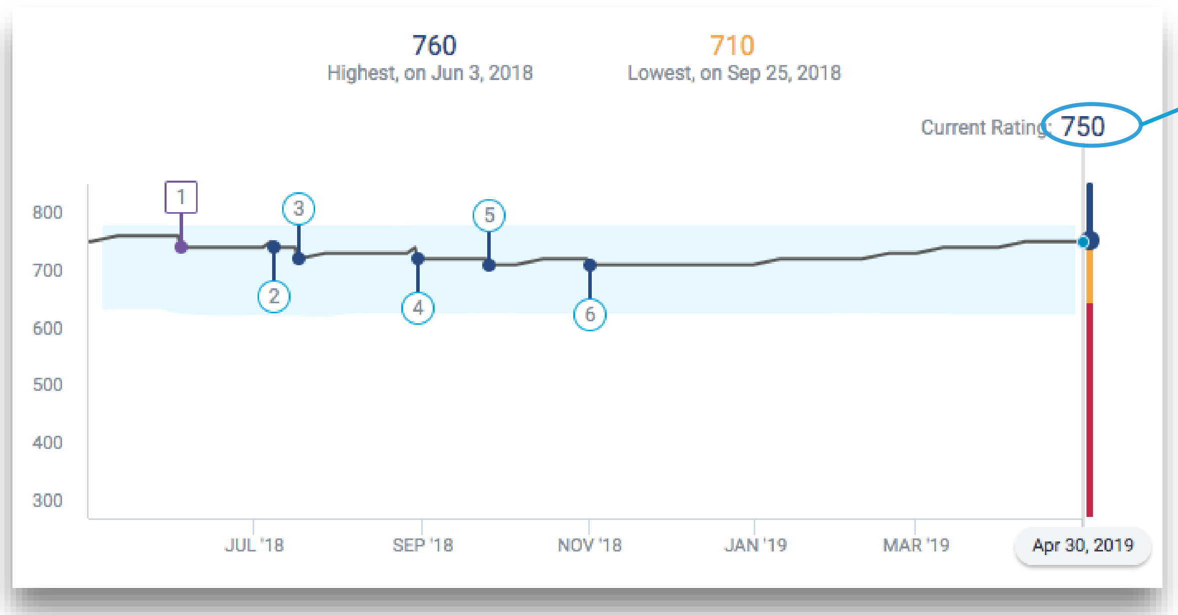
Source: Gartner (November 2018)

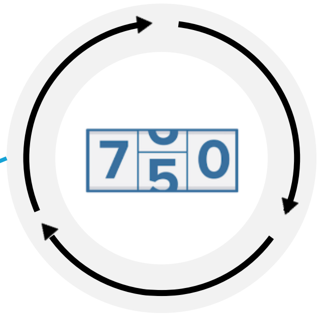
These graphics were published by Gartner, Inc. as part of larger research documents and should be evaluated in the context of the entire document. The Gartner documents are available upon request from ProcessUnity. Disclaimer: Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, and is used herein with permission. All rights reserved.

BitSight: Translate Complex Cybersecurity Issues into Simple Business Context

Objective, Continuous, Data-Driven Ratings of Organizational Security Performance



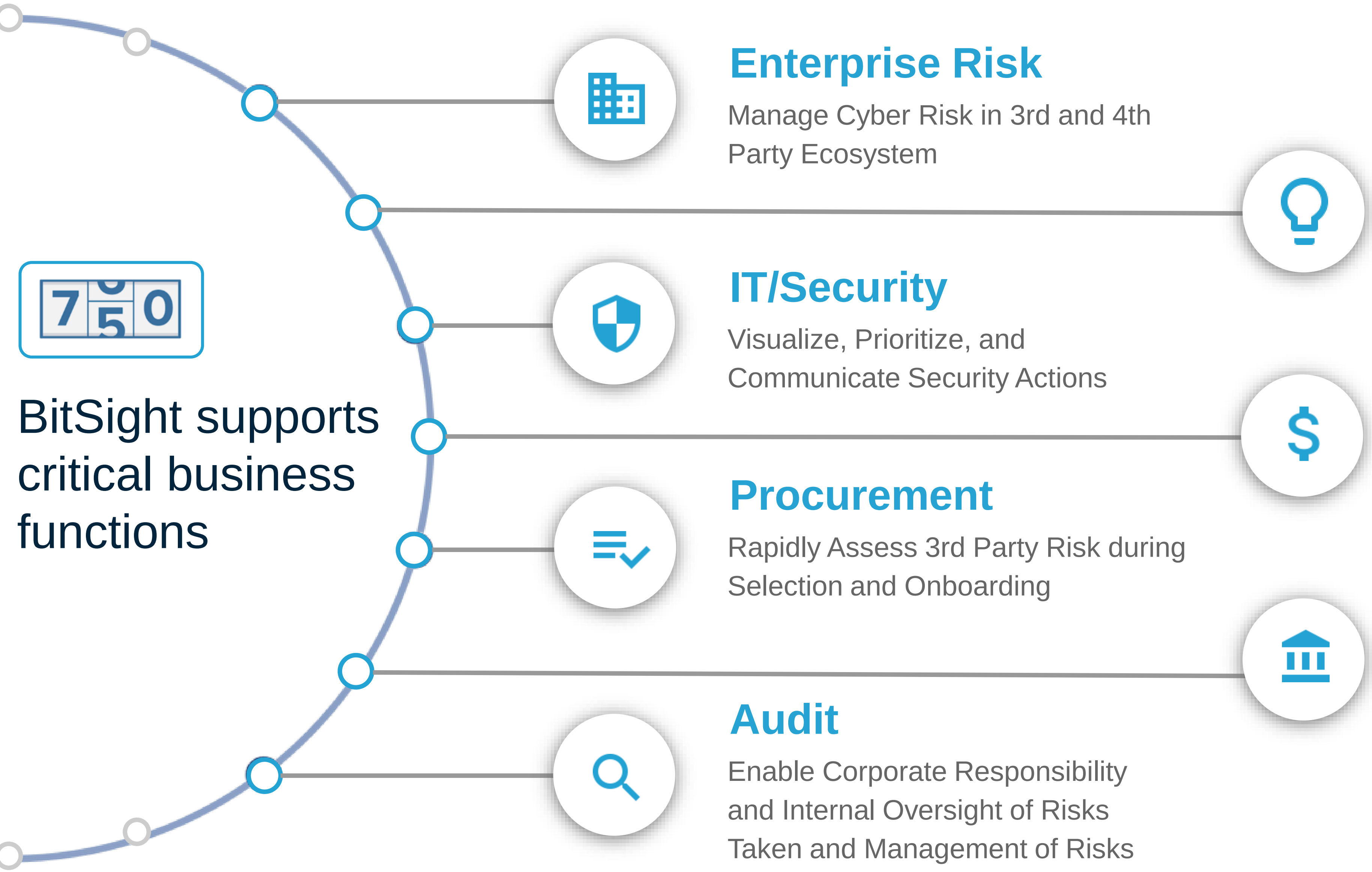


250 - 900

→ *Unbiased common* metric to measure cybersecurity performance of organizations worldwide

→ SaaS solution, ratings updated *daily*

...to Create a Common Language Across Enterprise...



BitSight supports critical business functions

Enterprise Risk

Manage Cyber Risk in 3rd and 4th Party Ecosystem

Marketing

Differentiate Against Competition with Effective Security Posture

IT/Security

Visualize, Prioritize, and Communicate Security Actions

Finance

Spend Effectively & Allocate/Prioritize Resources

Procurement

Rapidly Assess 3rd Party Risk during Selection and Onboarding

Legal

Objectively Evaluate Exposure and Actions Taken

Audit

Enable Corporate Responsibility and Internal Oversight of Risks Taken and Management of Risks

BITSIGHT®

BitSight: The Standard in Security Ratings

BITSIGHT®
The Standard in SECURITY RATINGS

BitSight provides an **independent rating of an organization’s cybersecurity performance.**

Methodology:

- Continuous, automated, non-intrusive collection of security evidence (200b+ events)
- Data-driven, objective rating of security performance

Gartner
peerinsights
customers’
choice
2020 ™

The BitSight ratings can be incorporated into an overall risk calculation inside of the ProcessUnity platform.

BITSIGHT®

The COVID-19 Pandemic

Principles for Preparing for and Responding to a Black Swan*

*Adapted from *Responding to a Black Swan*, Ernst & Young, 2011

Principles for Preparing for and Responding to a Black Swan*

Black Swan events may evolve from one factor or a combination of factors, including human error, negligence, malicious actions or acts of nature. Regardless of their cause, they are alike in that they:

- Occur unpredictably or unexpectedly
- Develop rapidly and continue for days, weeks, and even months
- Are catastrophic in scale and broad in scope
- Present hazards beyond immediate financial risks, jeopardizing lives, long-term health and the environment
- Involve significant asset damage or loss

*Adapted from *Responding to a Black Swan*, Ernst & Young, 2011

Responding to a Black Swan*

1. Develop risk recognition criteria in order to know when and how to respond.
2. Develop a quick response team led by a senior manager, typically the COO. This team should include personnel from across the business functions and external advisers. The team should concentrate on containing and minimizing the event.
3. Create a response team of leaders who should assess the situation, understand the risks faced, and response goals in order to quickly initiate the correct response plan.
4. Develop multiple response options and categorize them base on largest contribution toward response goals.
5. Evaluate each option by considering its risk/reward and whether the organization has the capabilities to carry out the plan. Critical assumptions should be documented during this process for future reference.
6. Complete an assessment of suppliers to ensure your suppliers' suppliers are not going to negatively impact your business.
7. Monitor your supply chain. Make sure that you are monitoring the risks associated with both your Tier 1 and Tier 2 suppliers to ensure your company has a complete view of the supply chain.
8. Identify alternative suppliers in non-impacted regions of the world to diversify the supply chain and limit dependencies on any one supplier of geographic region.
9. Assess continually the effectiveness of the response by making corrections as need.
10. After the event, management should discuss lessons learned and incorporate these lessons into training and future response planning.

*Adapted from *Responding to a Black Swan*, Ernst & Young, 2011

Responding to a Black Swan*

1. Develop risk recognition criteria in order to know when and how to respond.

2. Develop a quick response team led by a senior manager, typically the COO. This team should include personnel from across the business functions and external advisers. The team should concentrate on containing and minimizing the event.

3. Create a response team of leaders who should assess the situation, understand the risks faced, and response goals in order to quickly initiate the correct response plan.

4. Develop multiple response options and categorize them base on largest contribution toward response goals.

5. Evaluate each option by considering its risk/reward and whether the organization has the capabilities to carry out the plan. Critical assumptions should be documented during this process for future reference.

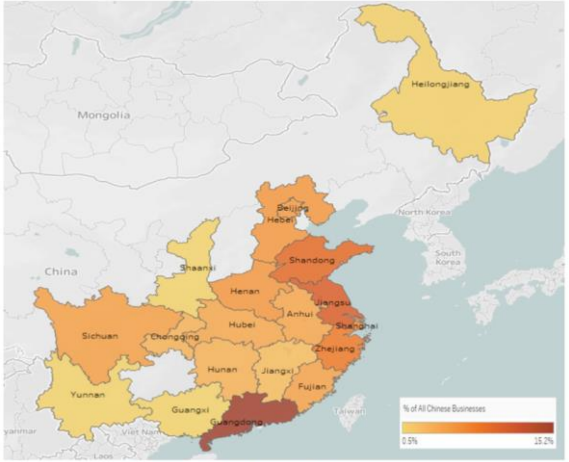
6. **Complete an assessment of suppliers to ensure your suppliers' suppliers are not going to negatively impact your business.**

7. Monitor your supply chain. Make sure that you are monitoring the risks associated with both your Tier 1 and Tier 2 suppliers to ensure your company has a complete view of the supply chain.

8. Identify alternative suppliers in non-impacted regions of the world to diversify the supply chain and limit dependencies on any one supplier of geographic region.

9. Assess continually the effectiveness of the response by making corrections as need.

10. After the event, management should discuss lessons learned and incorporate these lessons into training and future response planning.



Provinces with 100+ Confirmed Cases and Percent of All Chinese Businesses Affected

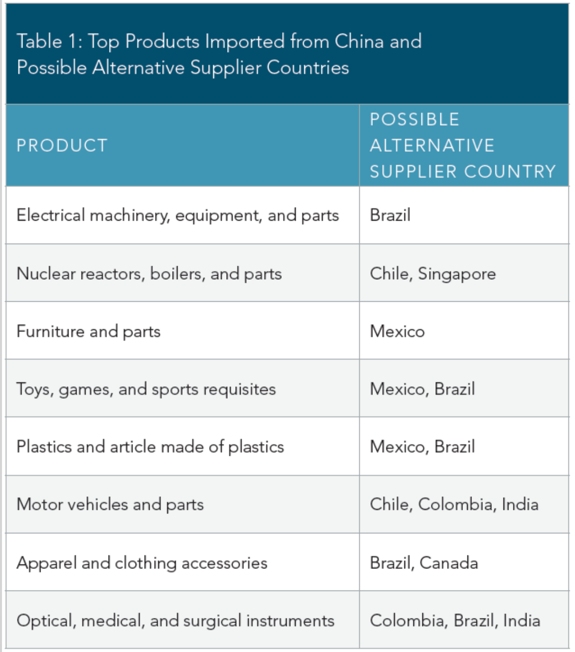


Table 1: Top Products Imported from China and Possible Alternative Supplier Countries

PRODUCT	POSSIBLE ALTERNATIVE SUPPLIER COUNTRY
Electrical machinery, equipment, and parts	Brazil
Nuclear reactors, boilers, and parts	Chile, Singapore
Furniture and parts	Mexico
Toys, games, and sports requisites	Mexico, Brazil
Plastics and article made of plastics	Mexico, Brazil
Motor vehicles and parts	Chile, Colombia, India
Apparel and clothing accessories	Brazil, Canada
Optical, medical, and surgical instruments	Colombia, Brazil, India

SOURCE: UN Comtrade and Dun & Bradstreet (February 5, 2020)

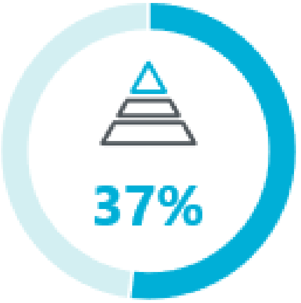
*Adapted from *Responding to a Black Swan*, Ernst & Young, 2011

Financial Impact of Disruptions

Supplier disruptions cost organizations time and money

Disruption is Pervasive and Impactful[1]

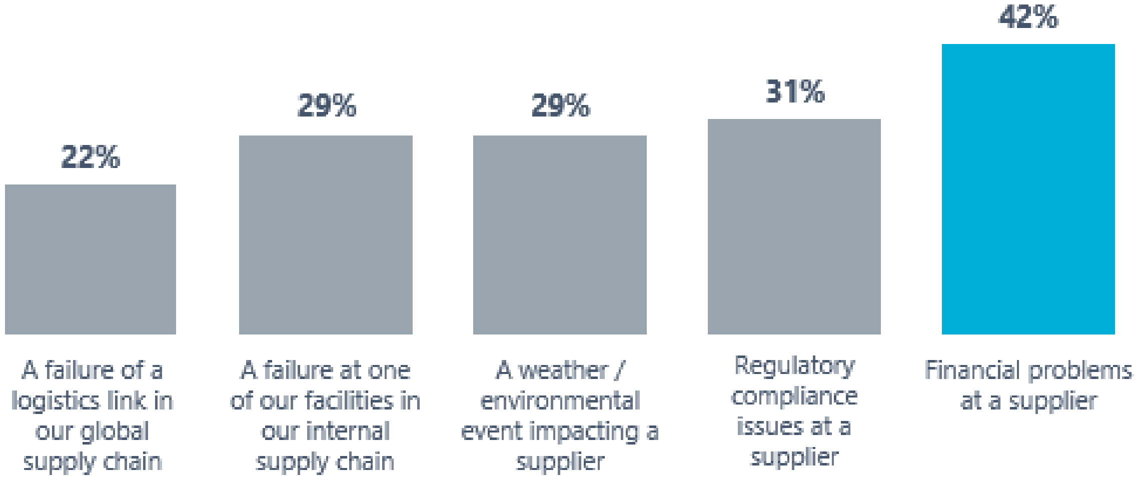
suffered a supply chain disruption in the past 12 months[3]



of disruptions occur at Tier 2 and beyond

1 in every 20 organization experiencing significant losses for a single disruption

Main Causes of Disruption[2]



1 - BCI (Business Continuity Institute). Supply Chain Resilience Report. 2019

2 – ProcureCon. Direct Benchmarking Survey

3- Extrapolation based on COVID-19 Pandemic distribution Jan 2020 – April 2020

Financial Impact of Disruptions

Supplier disruptions cost organizations time and money

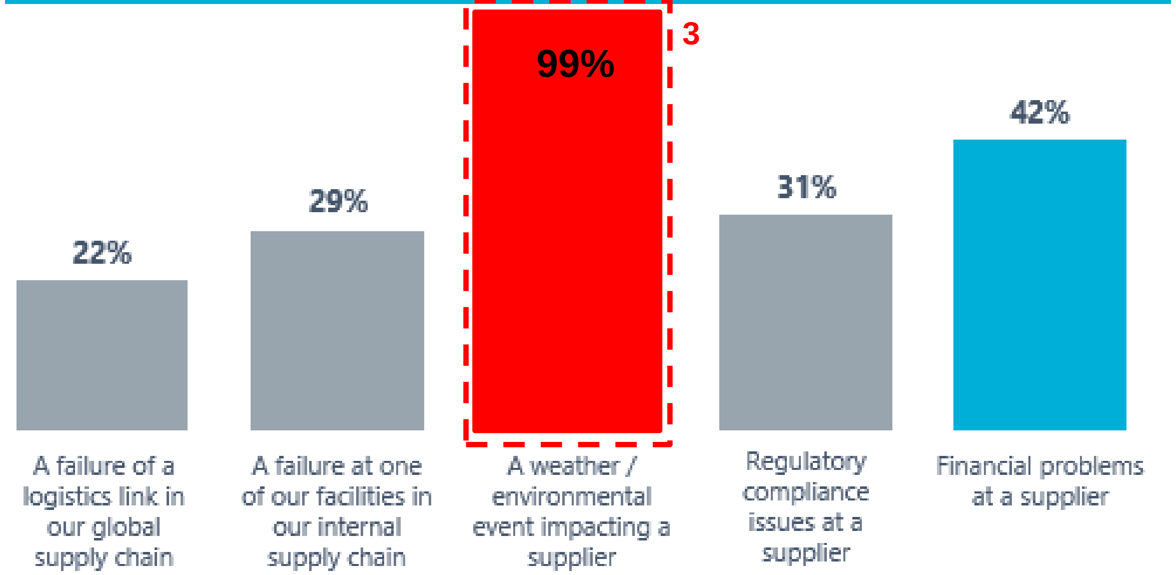
Disruption is Pervasive and Impactful[1]

100% suffered a supply chain disruption in the past 12 months[3]

37% of disruptions occur at Tier 2 and beyond

>$100M 1 in every 20 organization experiencing significant losses for a single disruption

Main Causes of Disruption[2]



[1] - BCI (Business Continuity Institute). Supply Chain Resilience Report. 2019

[2] – ProcureCon. Direct Benchmarking Survey

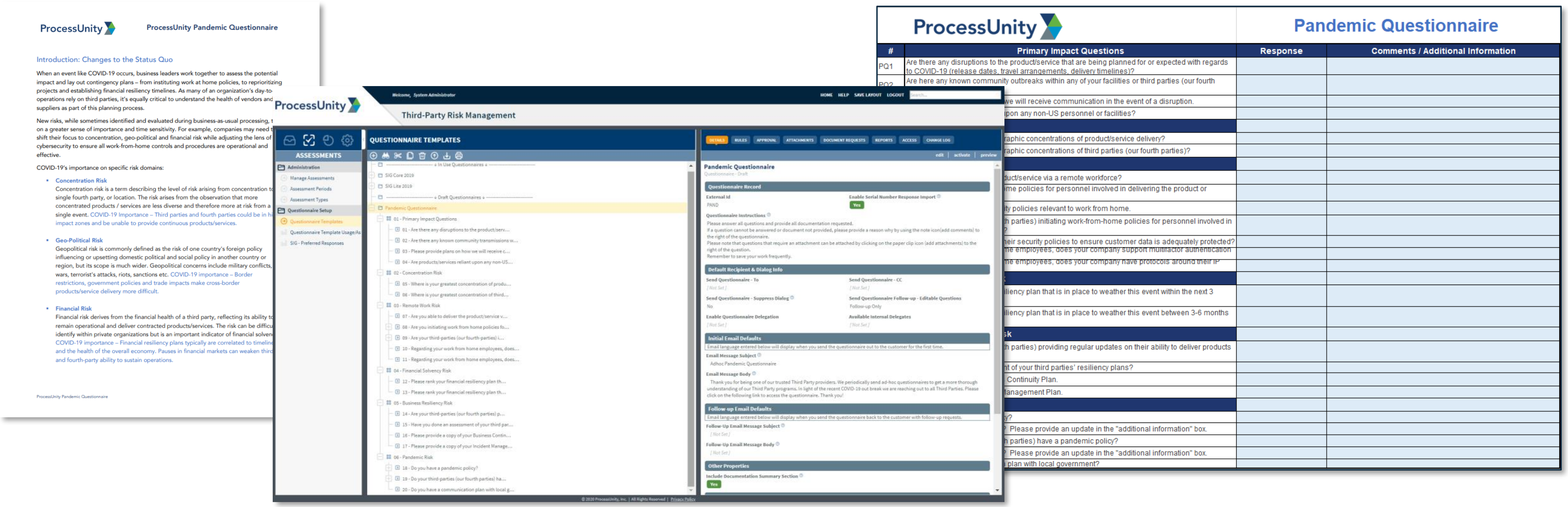
[3]- Extrapolation based on COVID-19 Pandemic distribution Jan 2020 – April 2020

…What a difference a month makes

ProcessUnity

ProcessUnity Response

- Immediate WFH business continuity exercise > WFH BAU
- Pandemic Questionnaire: Assess your Third-Party Network
  - Vet your critical and high-risk vendors



ProcessUnity Pandemic Questionnaire

Introduction: Changes to the Status Quo

When an event like COVID-19 occurs, business leaders work together to assess the potential impact and lay out contingency plans – from instituting work at home policies, to reprioritizing projects and establishing financial resiliency timelines. As many of an organization's day-to-operations rely on third parties, it's equally critical to understand the health of vendors and suppliers as part of this planning process.

New risks, while sometimes identified and evaluated during business-as-usual processing, t on a greater sense of importance and time sensitivity. For example, companies may need t shift their focus to concentration, geo-political and financial risk while adjusting the lens of cybersecurity to ensure all work-from-home controls and procedures are operational and effective.

COVID-19's importance on specific risk domains:

- **Concentration Risk**
  Concentration risk is a term describing the level of risk arising from concentration to single fourth party, or location. The risk arises from the observation that more concentrated products / services are less diverse and therefore more at risk from a single event. COVID-19 Importance – Third parties and fourth parties could be in hi impact zones and be unable to provide continuous products/services.
- **Geo-Political Risk**
  Geopolitical risk is commonly defined as the risk of one country's foreign policy influencing or upsetting domestic political and social policy in another country or region, but its scope is much wider. Geopolitical concerns include military conflicts, wars, terrorist's attacks, riots, sanctions etc. COVID-19 importance – Border restrictions, government policies and trade impacts make cross-border products/service delivery more difficult.
- **Financial Risk**
  Financial risk derives from the financial health of a third party, reflecting its ability to remain operational and deliver contracted products/services. The risk can be difficu identify within private organizations but is an important indicator of financial solven COVID-19 importance – Financial resiliency plans typically are correlated to timeline and the health of the overall economy. Pauses in financial markets can weaken third and fourth-party ability to sustain operations.

ProcessUnity Pandemic Questionnaire

Welcome, System Administrator

HOME HELP SAVE LAYOUT LOGOUT Search...

Third-Party Risk Management

ASSESSMENTS

- Administration
  - Manage Assessments
  - Assessment Periods
  - Assessment Types
- Questionnaire Setup
  - Questionnaire Templates
  - Questionnaire Template Usage/As
  - SIG - Preferred Responses

QUESTIONNAIRE TEMPLATES

- ↓ In Use Questionnaires ↓
- SIG Core 2019
- SIG Lite 2019
- ↓ Draft Questionnaires ↓
- Pandemic Questionnaire
  - 01 - Primary Impact Questions
    - 01 - Are there any disruptions to the product/serv...
    - 02 - Are there any known community transmissions w...
    - 03 - Please provide plans on how we will receive c...
    - 04 - Are products/services reliant upon any non-US...
  - 02 - Concentration Risk
    - 05 - Where is your greatest concentration of produ...
    - 06 - Where is your greatest concentration of third...
  - 03 - Remote Work Risk
    - 07 - Are you able to deliver the product/service v...
    - 08 - Are you initiating work from home policies fo...
    - 09 - Are your third-parties (our fourth-parties) i...
    - 10 - Regarding your work from home employees, does...
    - 11 - Regarding your work from home employees, does...
  - 04 - Financial Solvency Risk
    - 12 - Please rank your financial resiliency plan th...
    - 13 - Please rank your financial resiliency plan th...
  - 05 - Business Resiliency Risk
    - 14 - Are your third-parties (our fourth parties) p...
    - 15 - Have you done an assessment of your third par...
    - 16 - Please provide a copy of your Business Contin...
    - 17 - Please provide a copy of your Incident Manage...
  - 06 - Pandemic Risk
    - 18 - Do you have a pandemic policy?
    - 19 - Do your third-parties (our fourth parties) ha...
    - 20 - Do you have a communication plan with local g...

DETAILS RULES APPROVAL ATTACHMENTS DOCUMENT REQUESTS REPORTS ACCESS CHANGE LOG

edit | activate | preview

Pandemic Questionnaire
Questionnaire - Draft

Questionnaire Record

External Id: PAND

Enable Serial Number Response Import: Yes

Questionnaire Instructions:
Please answer all questions and provide all documentation requested.
If a question cannot be answered or document not provided, please provide a reason why by using the note icon(add comments) to the right of the questionnaire.
Please note that questions that require an attachment can be attached by clicking on the paper clip icon (add attachments) to the right of the question.
Remember to save your work frequently.

Default Recipient & Dialog Info

Send Questionnaire - To: [Not Set]

Send Questionnaire - CC: [Not Set]

Send Questionnaire - Suppress Dialog: No

Send Questionnaire Follow-up - Editable Questions: Follow-up Only

Enable Questionnaire Delegation: [Not Set]

Available Internal Delegates: [Not Set]

Initial Email Defaults

Email language entered below will display when you send the questionnaire out to the customer for the first time.

Email Message Subject: Adhoc Pandemic Questionnaire

Email Message Body:
Thank you for being one of our trusted Third Party providers. We periodically send ad-hoc questionnaires to get a more thorough understanding of our Third Party programs. In light of the recent COVID-19 out break we are reaching out to all Third Parties. Please click on the following link to access the questionnaire. Thank you!

Follow-up Email Defaults

Email language entered below will display when you send the questionnaire back to the customer with follow-up requests.

Follow-Up Email Message Subject: [Not Set]

Follow-Up Email Message Body: [Not Set]

Other Properties

Include Documentation Summary Section: Yes

© 2020 ProcessUnity, Inc. | All Rights Reserved | Privacy Policy

Pandemic Questionnaire

#	Primary Impact Questions	Response	Comments / Additional Information
PQ1	Are there any disruptions to the product/service that are being planned for or expected with regards to COVID-19 (release dates, travel arrangements, delivery timelines)?		
PQ2	Are here any known community outbreaks within any of your facilities or third parties (our fourth		
	we will receive communication in the event of a disruption.		
	pon any non-US personnel or facilities?		
	raphic concentrations of product/service delivery?		
	raphic concentrations of third parties (our fourth parties)?		
	duct/service via a remote workforce?		
	me policies for personnel involved in delivering the product or		
	ty policies relevant to work from home.		
	h parties) initiating work-from-home policies for personnel involved in ?		
	heir security policies to ensure customer data is adequately protected?		
	me employees, does your company support multifactor authentication		
	me employees, does your company have protocols around their IP		
	k		
	liency plan that is in place to weather this event within the next 3		
	liency plan that is in place to weather this event between 3-6 months		
	sk		
	h parties) providing regular updates on their ability to deliver products		
	nt of your third parties' resiliency plans?		
	Continuity Plan.		
	lanagement Plan.		
	y?		
	Please provide an update in the "additional information" box.		
	h parties) have a pandemic policy?		
	Please provide an update in the "additional information" box.		
	plan with local government?		

Getting the House in Order

Re-assessing your TPRM building blocks

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

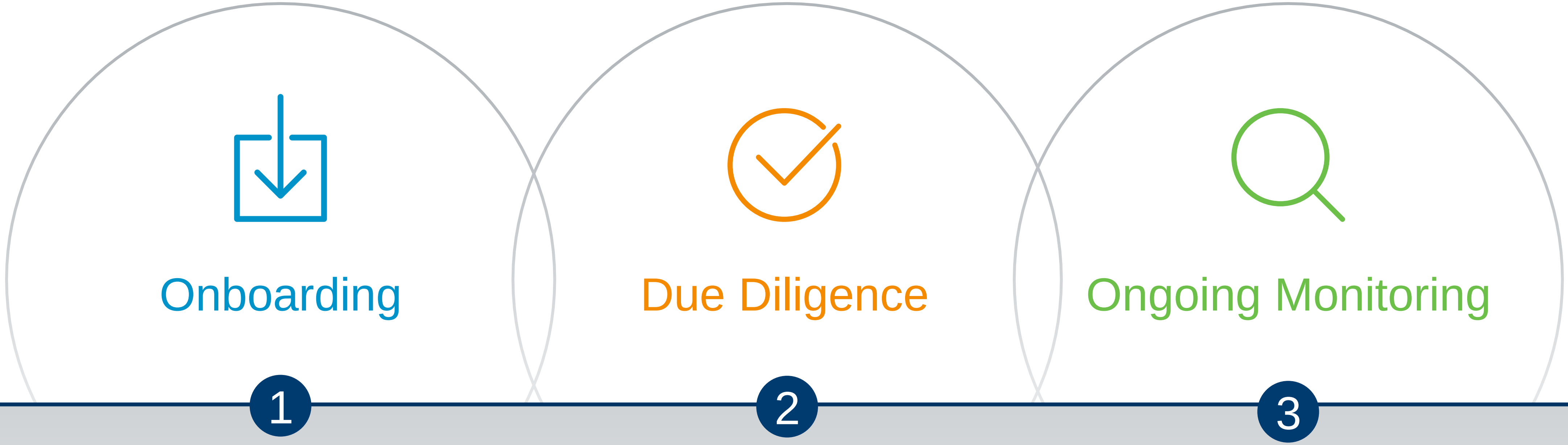
Issue Management

Formally track vendor issues

ProcessUnity

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

ProcessUnity

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

Critical Vendors — 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?

Framework & Process — 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?

Documentation — Storing Supporting Documentation

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

Nth Parties — 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?

ProcessUnity

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

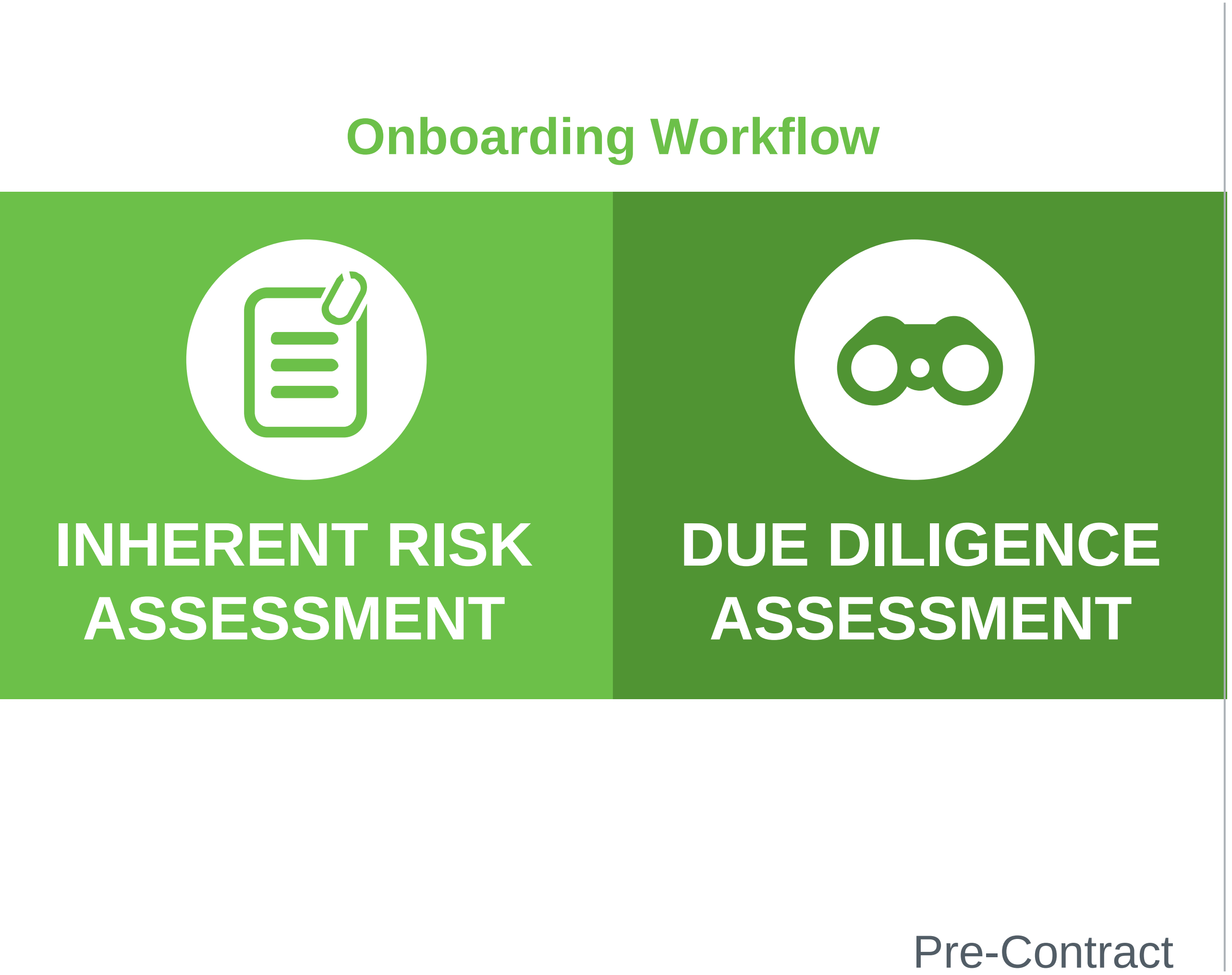
Building Blocks: Base Processes & Flows

Building Blocks: Base Processes & Flows

Pre-Contract

Post-Contract

Building Blocks: Base Processes & Flows



Onboarding Workflow

INHERENT RISK ASSESSMENT

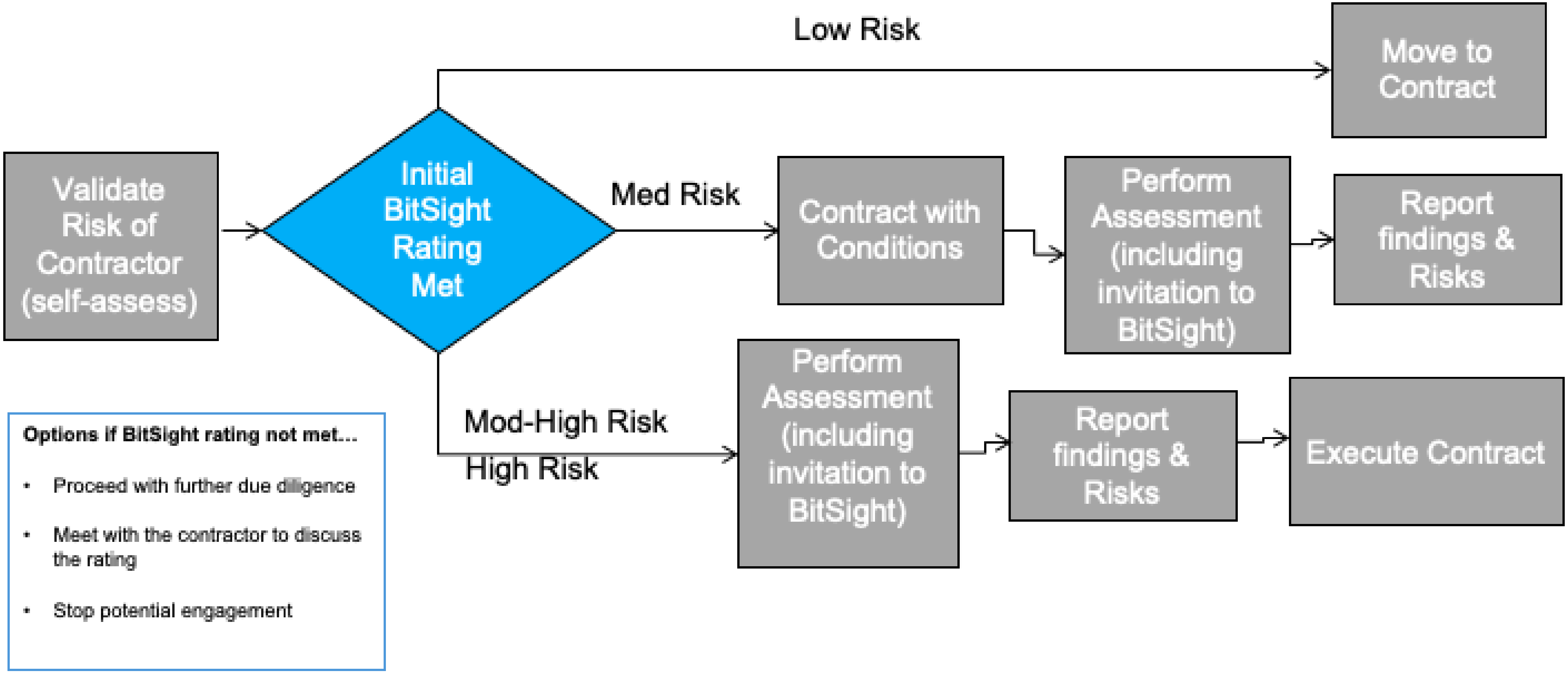
DUE DILIGENCE ASSESSMENT

Pre-Contract

Post-Contract

ProcessUnity

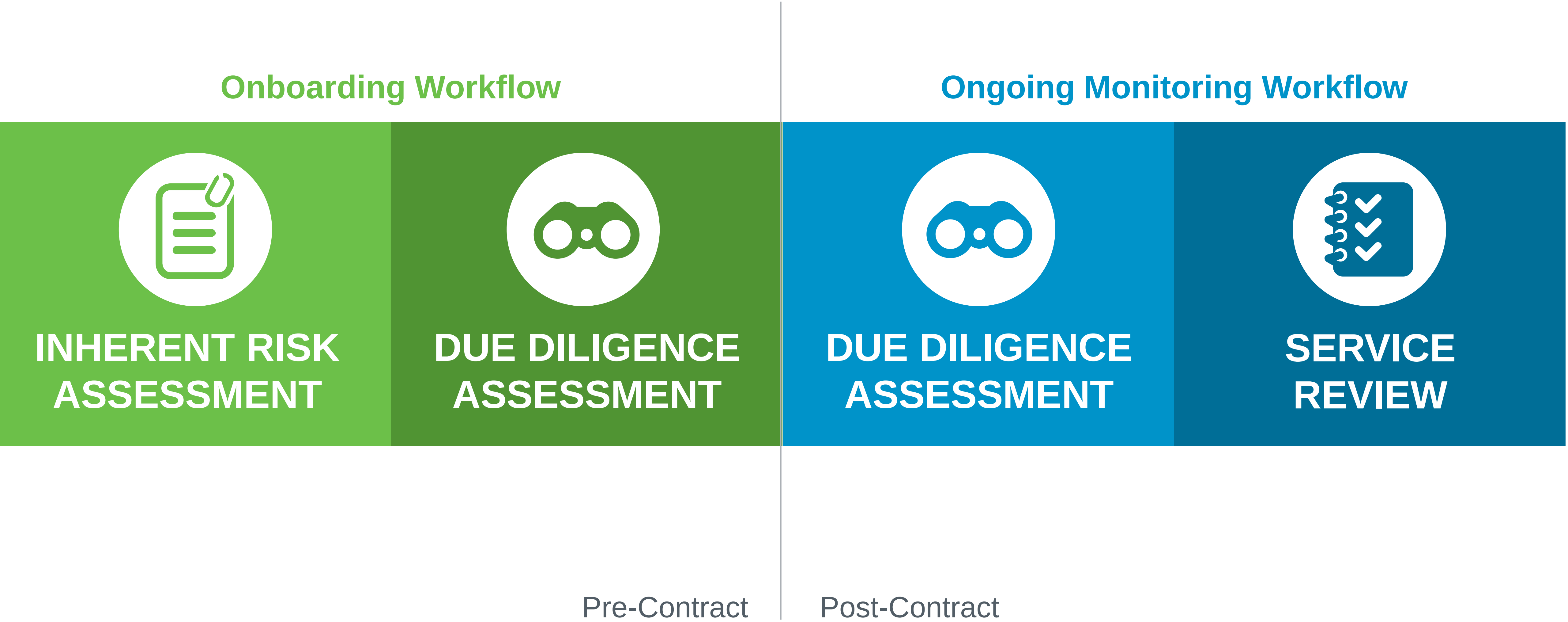
Moving Quickly to Meet Business Needs


Validate Risk of Contractor (self-assess)
Initial BitSight Rating Met
Low Risk
Move to Contract
Med Risk
Contract with Conditions
Perform Assessment (including invitation to BitSight)
Report findings & Risks
Mod-High Risk
High Risk
Perform Assessment (including invitation to BitSight)
Report findings & Risks
Execute Contract

Options if BitSight rating not met…

- Proceed with further due diligence
- Meet with the contractor to discuss the rating
- Stop potential engagement

Building Blocks: Base Processes & Flows



Onboarding Workflow

INHERENT RISK ASSESSMENT

DUE DILIGENCE ASSESSMENT

Ongoing Monitoring Workflow

DUE DILIGENCE ASSESSMENT

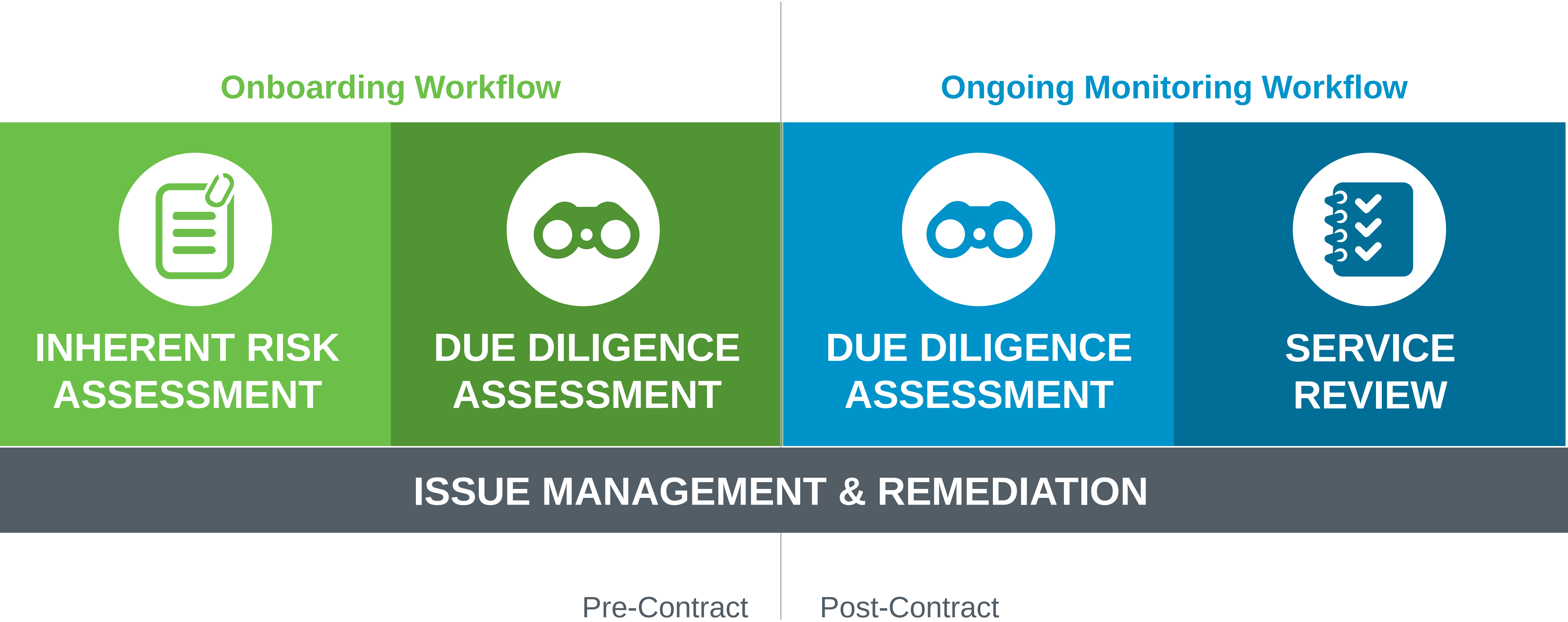
SERVICE REVIEW

Pre-Contract

Post-Contract

ProcessUnity

Building Blocks: Base Processes & Flows



Onboarding Workflow

Ongoing Monitoring Workflow

INHERENT RISK ASSESSMENT

DUE DILIGENCE ASSESSMENT

DUE DILIGENCE ASSESSMENT

SERVICE REVIEW

ISSUE MANAGEMENT & REMEDIATION

Pre-Contract

Post-Contract

ProcessUnity

Enriching the Third-Party Risk Management Workflows

ProcessUnity

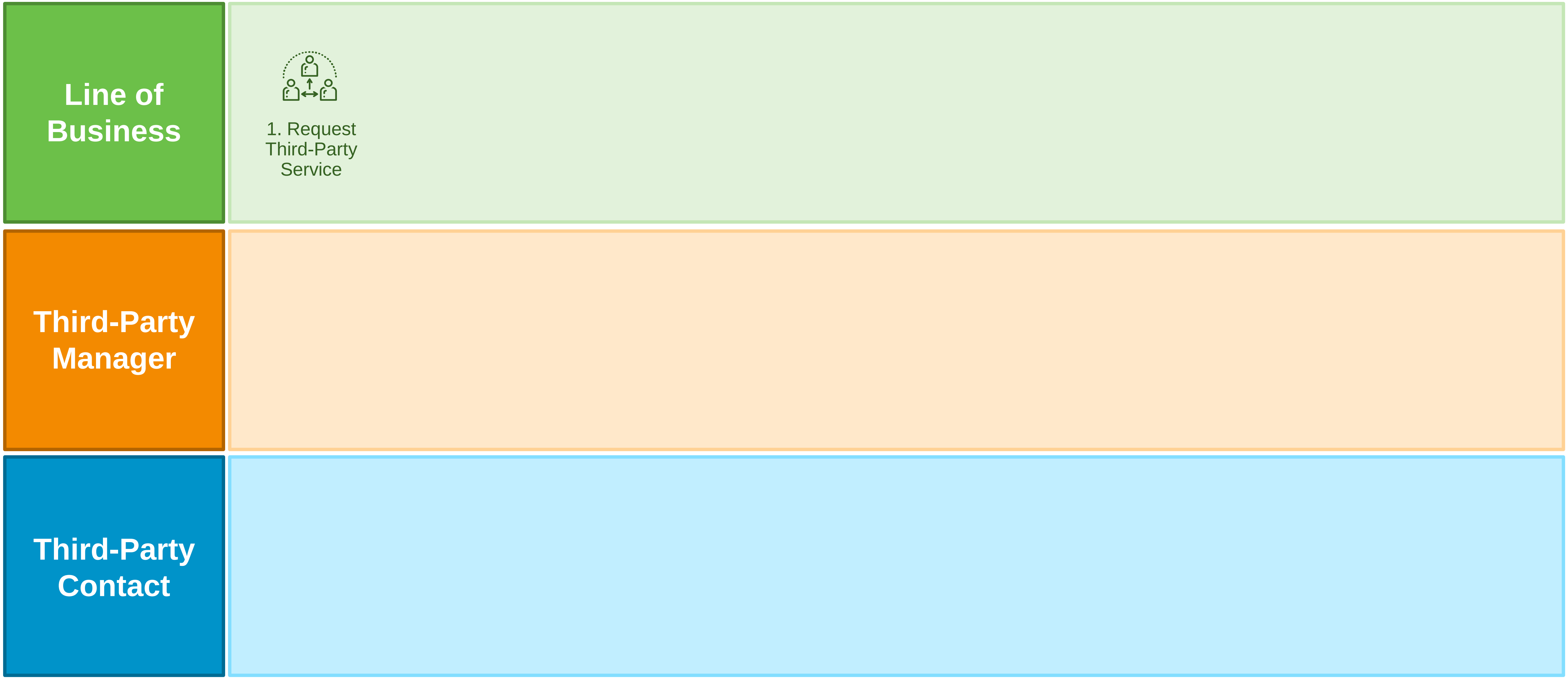
Onboarding Workflow

Line of Business

Third-Party Manager

Third-Party Contact

Onboarding Workflow



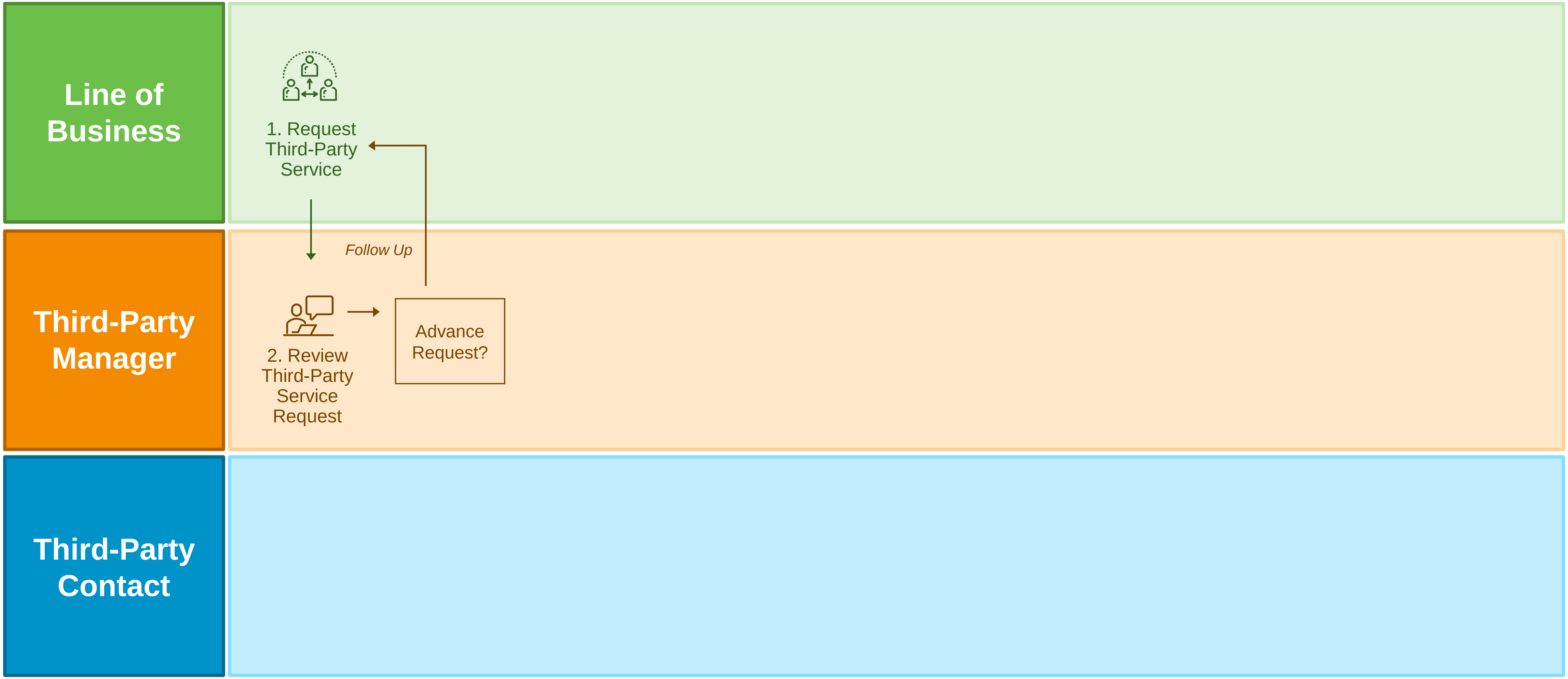
Line of Business

1. Request Third-Party Service

Third-Party Manager

Third-Party Contact

Onboarding Workflow



Line of Business

Third-Party Manager

Third-Party Contact

1. Request Third-Party Service

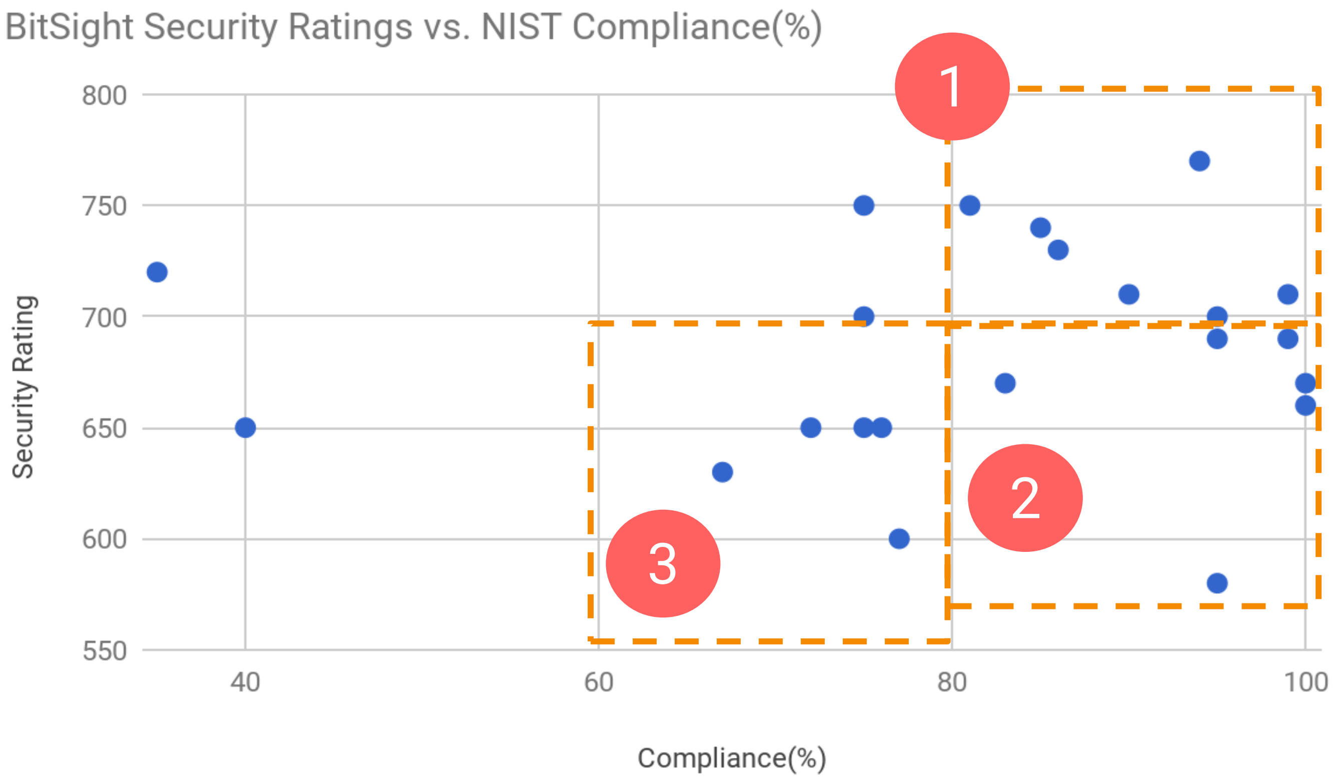
Follow Up

2. Review Third-Party Service Request

Advance Request?

ProcessUnity

Leveraging Security Ratings & Questionnaires



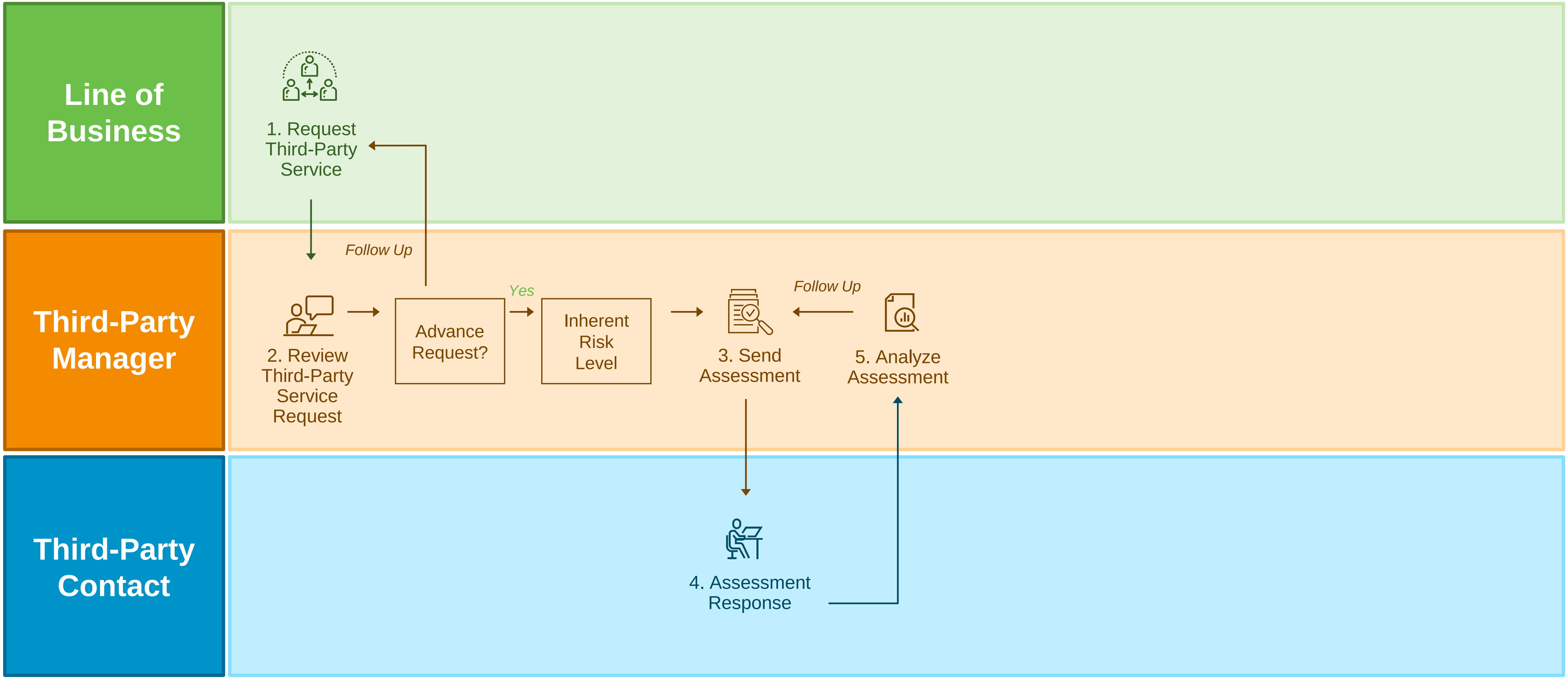
Security ratings + questionnaire response can validate responses and prioritize remediation efforts.

Monitor companies with ratings above 700 and a compliance rate above 80% 1

Organizations with low ratings and high compliance are natural candidates for follow-up 2

Direct remediation for low rating and low self-assessment 3

Onboarding Workflow



Line of Business

1. Request Third-Party Service

Third-Party Manager

2. Review Third-Party Service Request

Follow Up

Advance Request?

Yes

Inherent Risk Level

3. Send Assessment

Follow Up

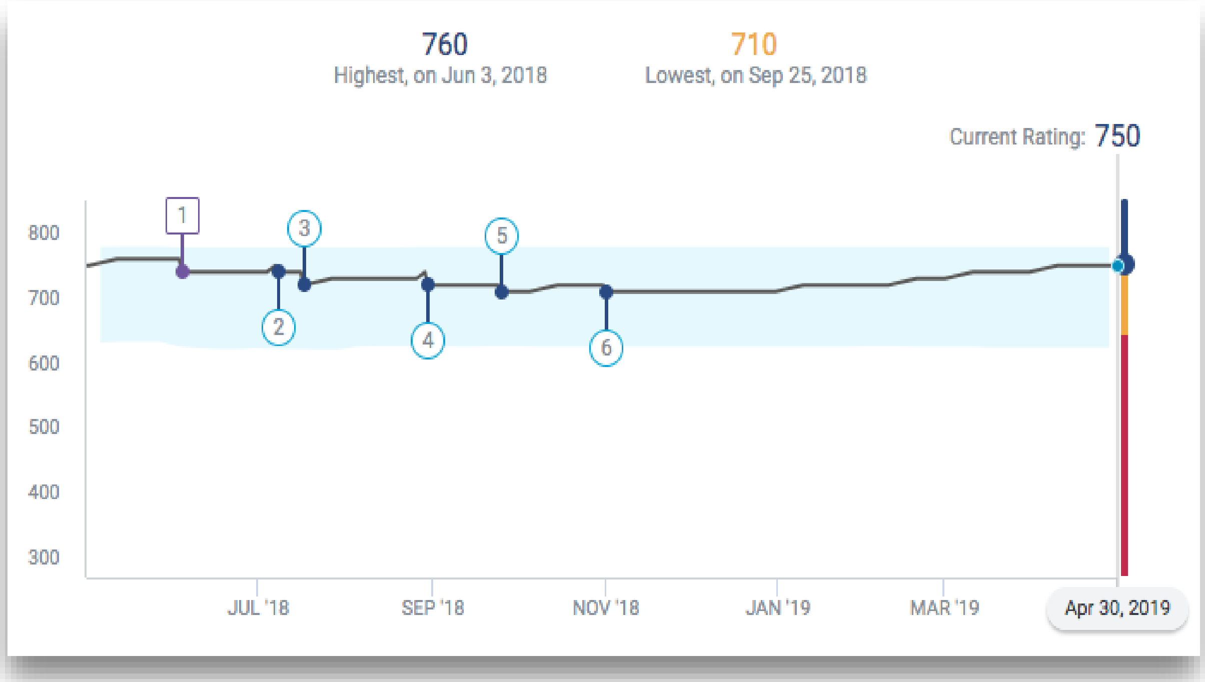
5. Analyze Assessment

Third-Party Contact

4. Assessment Response

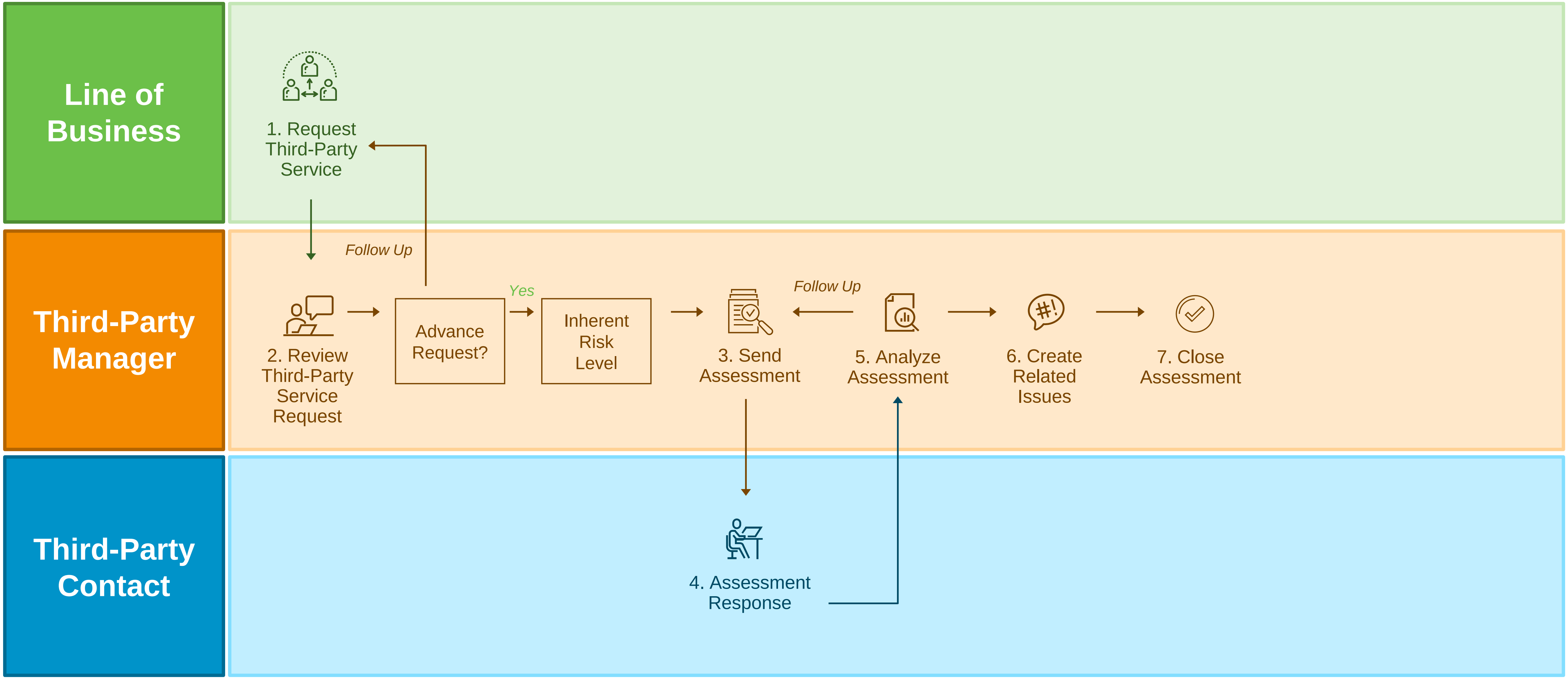
ProcessUnity

Trust but Validate



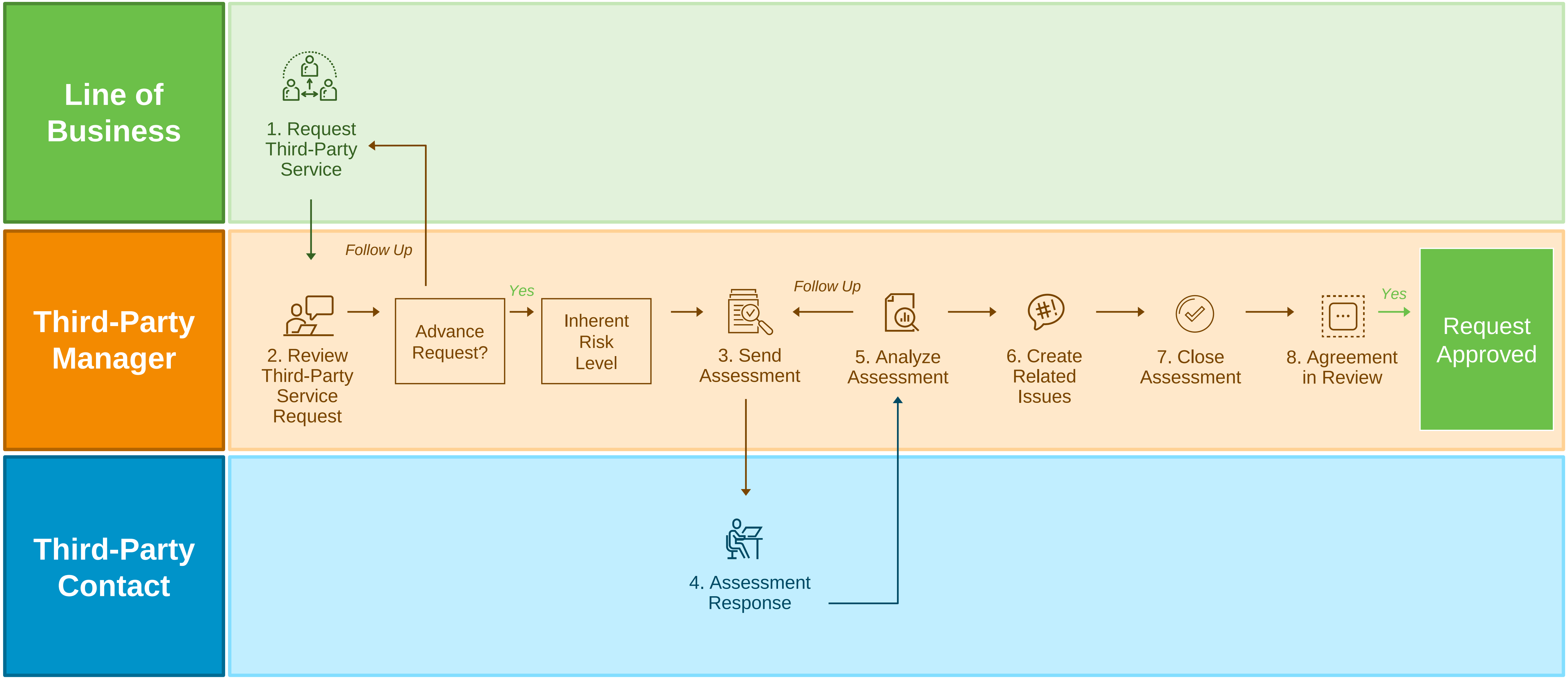
- ➔ *Rating platforms continuously monitor vendors for changes in cyber security posture; engage with vendors on an event driven basis (in addition to a calendar driven basis).*
- ➔ *Engage with vendors on remediation efforts with specific data and observations.*

Onboarding Workflow



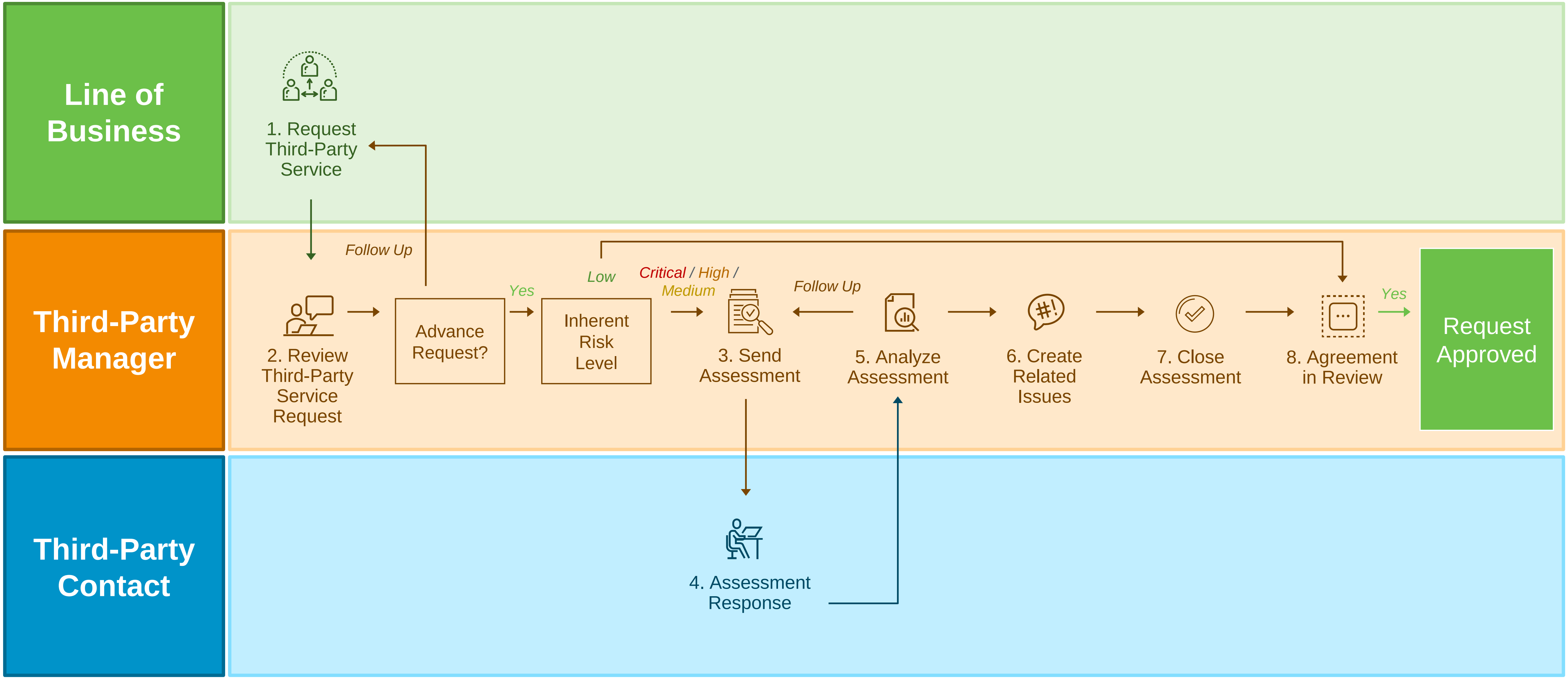
ProcessUnity

Onboarding Workflow



ProcessUnity

Onboarding Workflow



Line of Business

Third-Party Manager

Third-Party Contact

1. Request Third-Party Service

Follow Up

2. Review Third-Party Service Request

Advance Request?

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

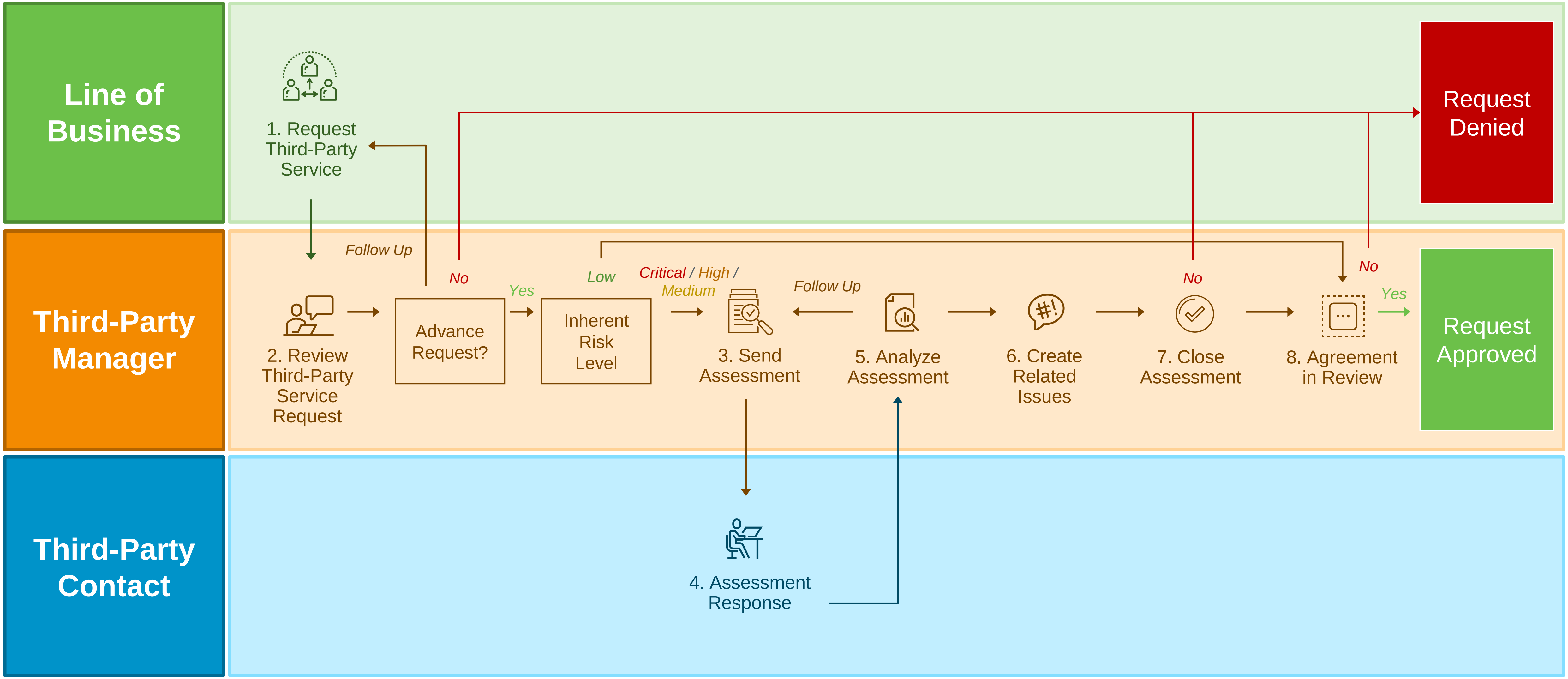
8. Agreement in Review

Yes

Request Approved

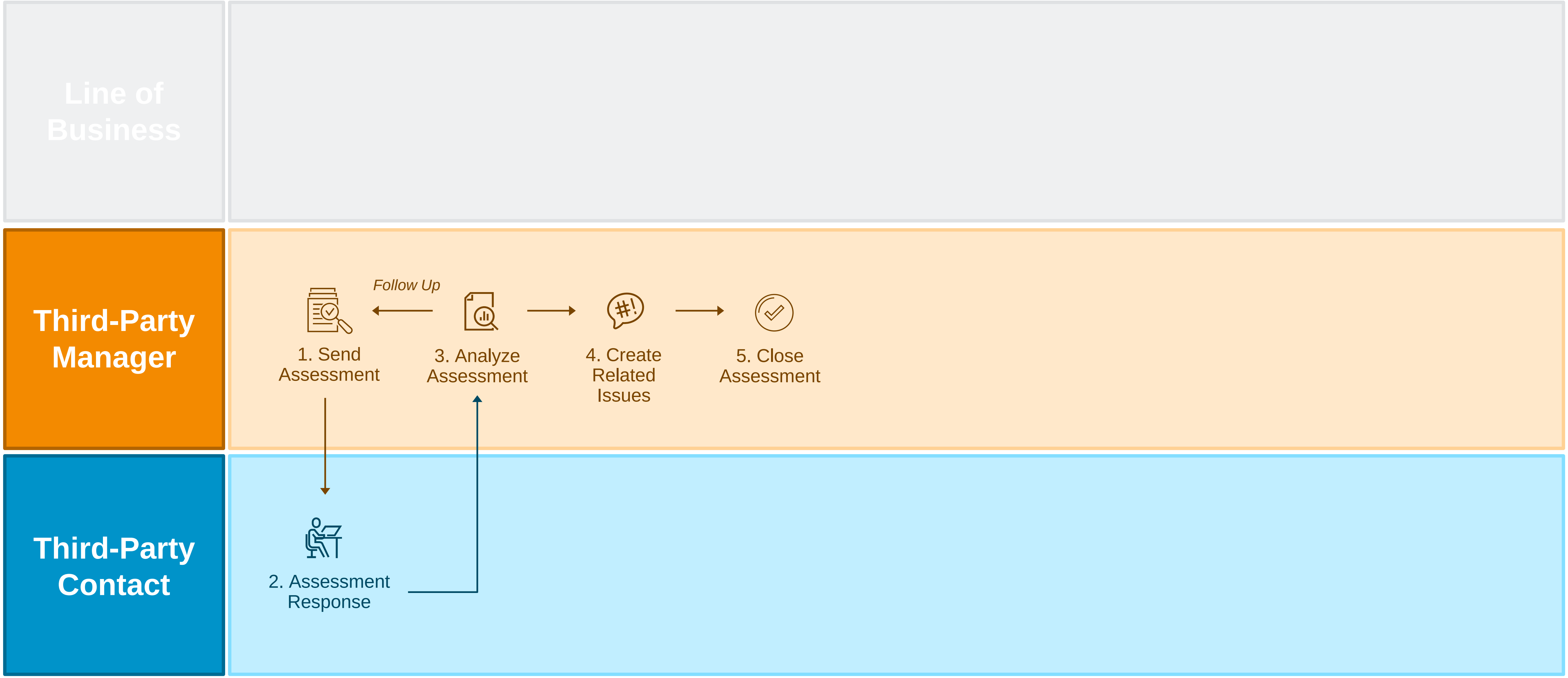
ProcessUnity

Onboarding Workflow



ProcessUnity

Ongoing Monitoring: Periodic Due Diligence



Line of Business

Third-Party Manager

1. Send Assessment

Follow Up

3. Analyze Assessment

4. Create Related Issues

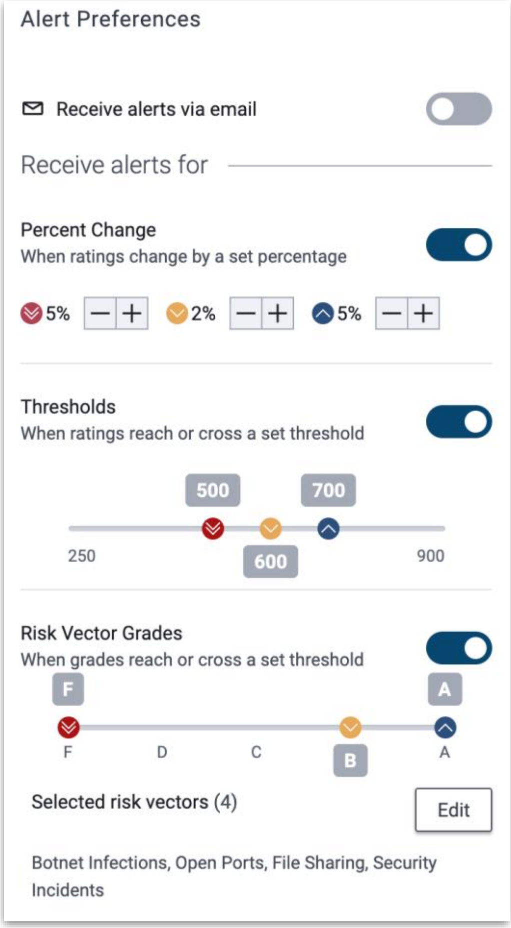
5. Close Assessment

Third-Party Contact

2. Assessment Response

Continuously Monitor

BitSight Alerts



Alert Preferences

Receive alerts via email

Receive alerts for

Percent Change
When ratings change by a set percentage

5% — + 2% — + 5% — +

Thresholds
When ratings reach or cross a set threshold

Risk Vector Grades
When grades reach or cross a set threshold

Selected risk vectors (4) Edit

Botnet Infections, Open Ports, File Sharing, Security Incidents

Manage by Exception

- Alerts by Tier
- Rating % Change
- Specific Risk Vectors

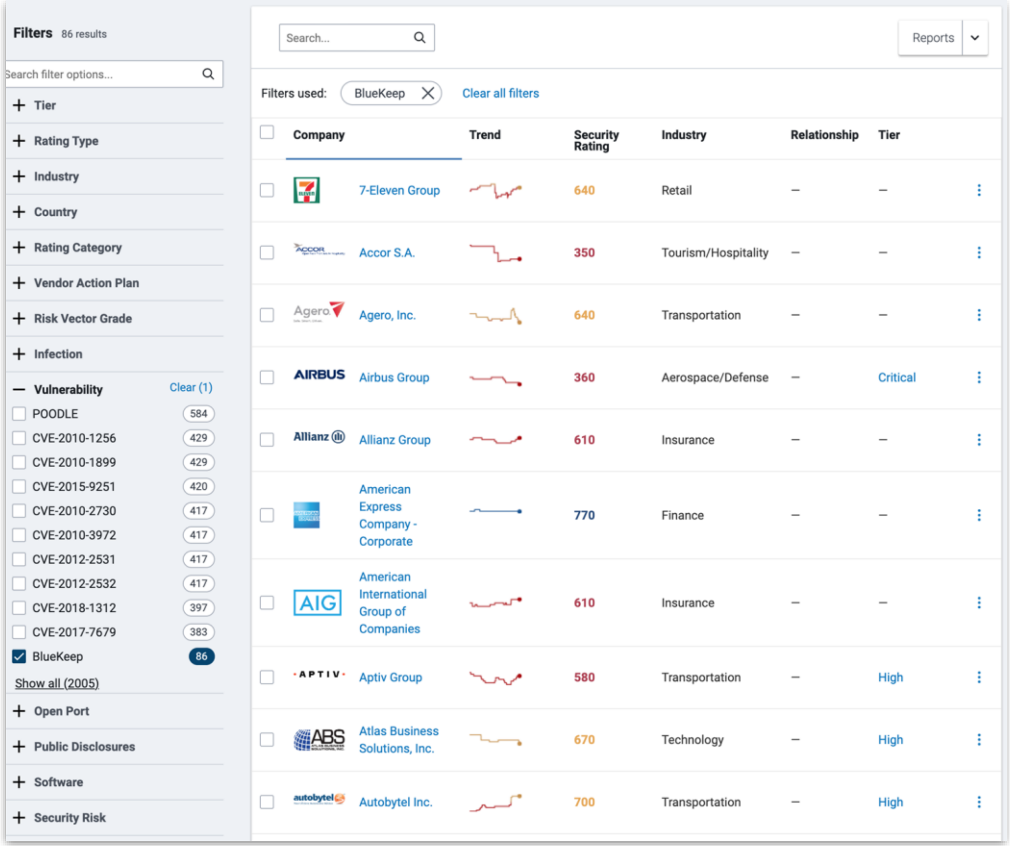
Communication Process

- Preliminary Introduction and Explanation
- EVA/email and Intro Call
- Include BitSight CSM

Remediation

- Vendor Access Dashboard
- Issues Management in GRC
- Escalations to Business when necessary

Risk Hunting



Filters 86 results

Search filter options...

- Tier
- Rating Type
- Industry
- Country
- Rating Category
- Vendor Action Plan
- Risk Vector Grade
- Infection

— Vulnerability Clear (1)

□ POODLE	584
□ CVE-2010-1256	429
□ CVE-2010-1899	429
□ CVE-2015-9251	420
□ CVE-2010-2730	417
□ CVE-2010-3972	417
□ CVE-2012-2531	417
□ CVE-2012-2532	417
□ CVE-2018-1312	397
□ CVE-2017-7679	383
☑ BlueKeep	86

Show all (2005)

- Open Port
- Public Disclosures
- Software
- Security Risk

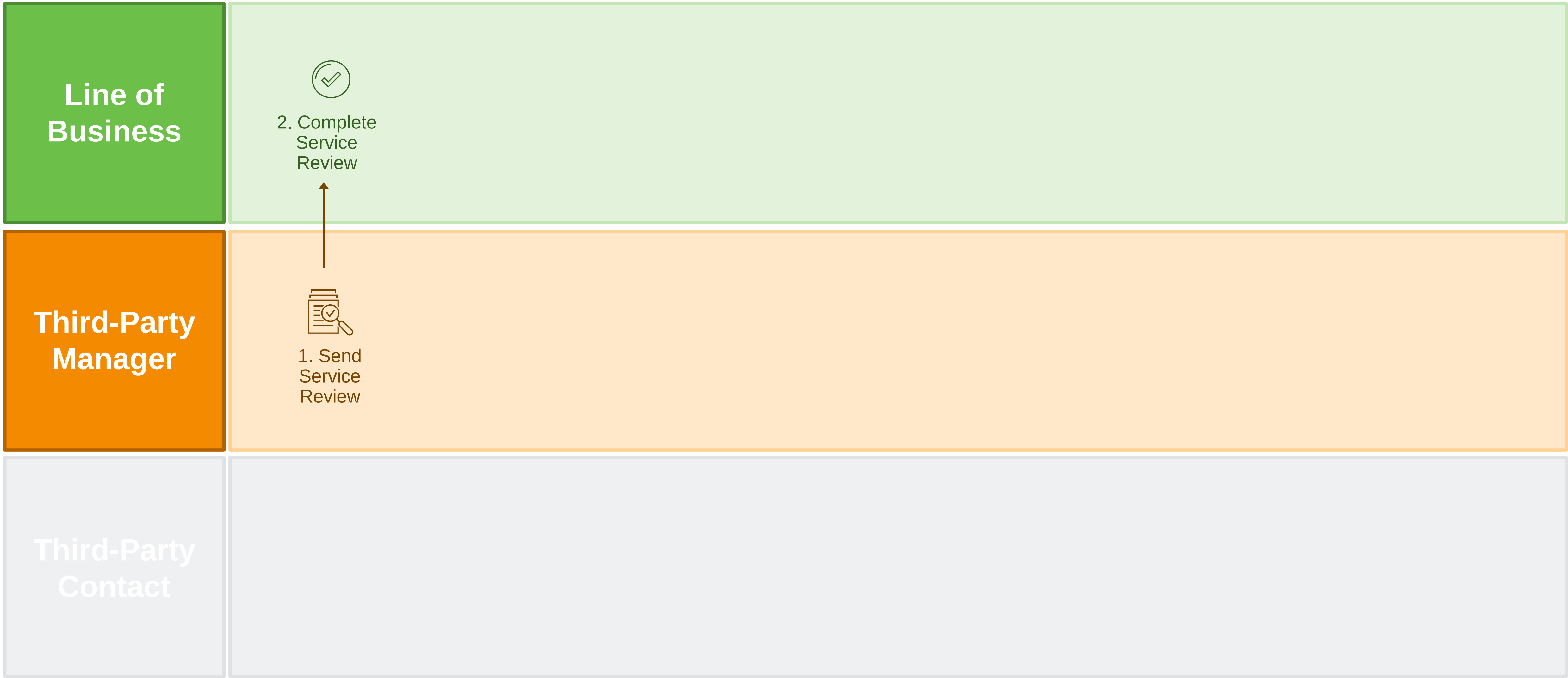
Search...

Reports

Filters used: BlueKeep ✕ Clear all filters

□	Company	Trend	Security Rating	Industry	Relationship	Tier
□	7-Eleven Group		640	Retail	–	–
□	Accor S.A.		350	Tourism/Hospitality	–	–
□	Agero, Inc.		640	Transportation	–	–
□	Airbus Group		360	Aerospace/Defense	–	Critical
□	Allianz Group		610	Insurance	–	–
□	American Express Company - Corporate		770	Finance	–	–
□	American International Group of Companies		610	Insurance	–	–
□	Aptiv Group		580	Transportation	–	High
□	Atlas Business Solutions, Inc.		670	Technology	–	High
□	Autobytel Inc.		700	Transportation	–	High

Ongoing Monitoring: Service Reviews



Line of Business

2. Complete Service Review

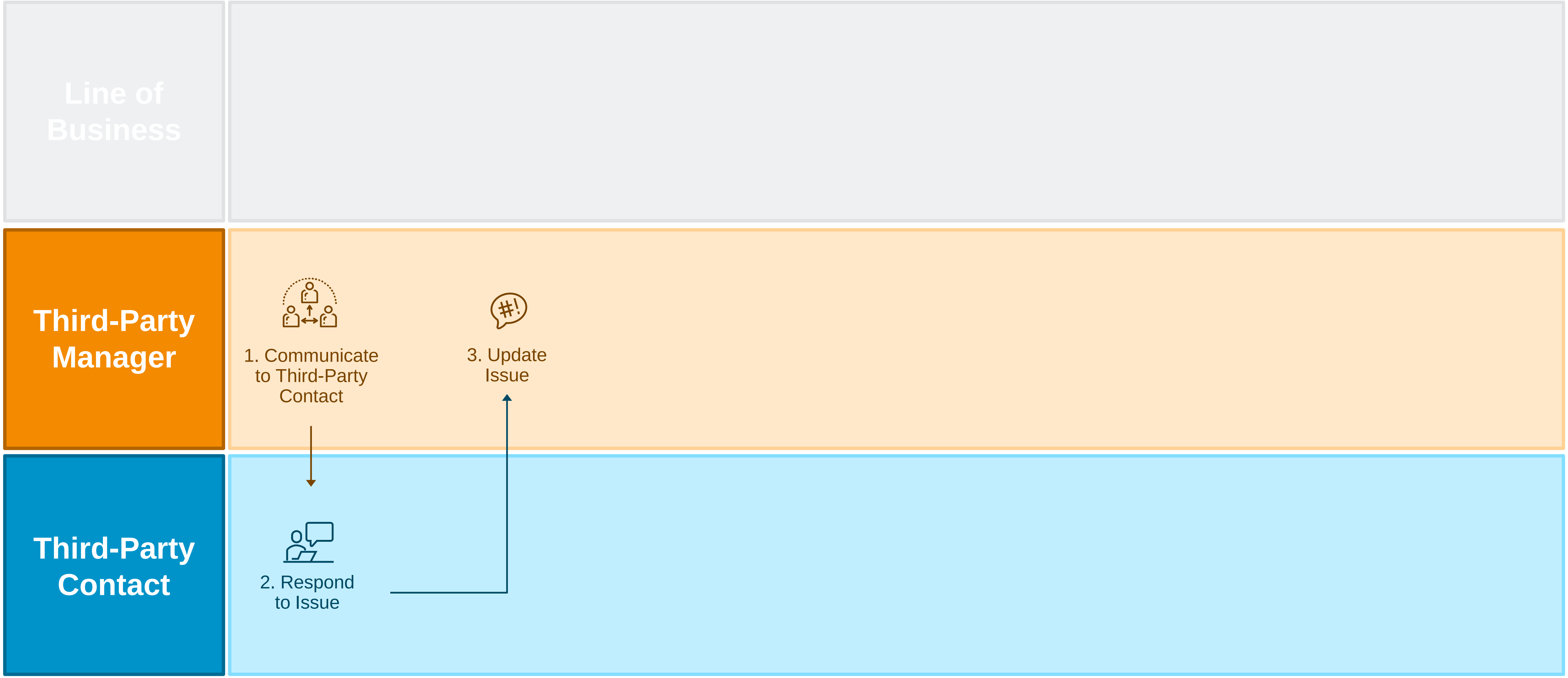
Third-Party Manager

1. Send Service Review

Third-Party Contact

ProcessUnity

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

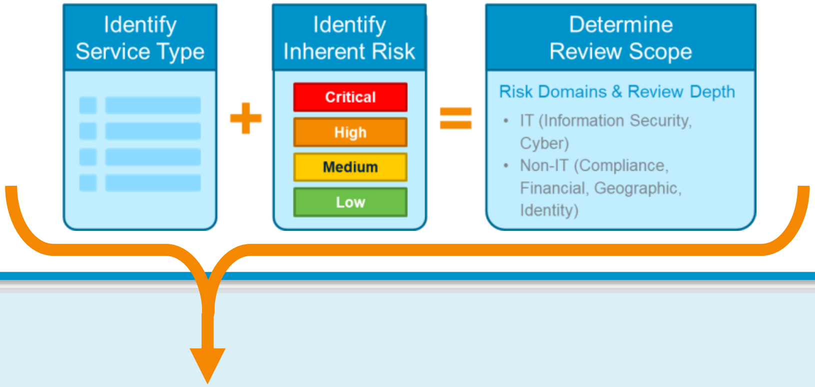
Own the Risk
Share the Responsibility

You Own the Risk (but you can accelerate the review)

Establish an Embedded TPRM Process

Define onboarding and ongoing monitoring activities.

- Inherent Risk Assessment and Scope
- Review Process and Data Analysis (Residual Risk)
- Cadence and Monitoring (Continuous, Contractual)



Identify Service Type + Identify Inherent Risk = Determine Review Scope

Critical

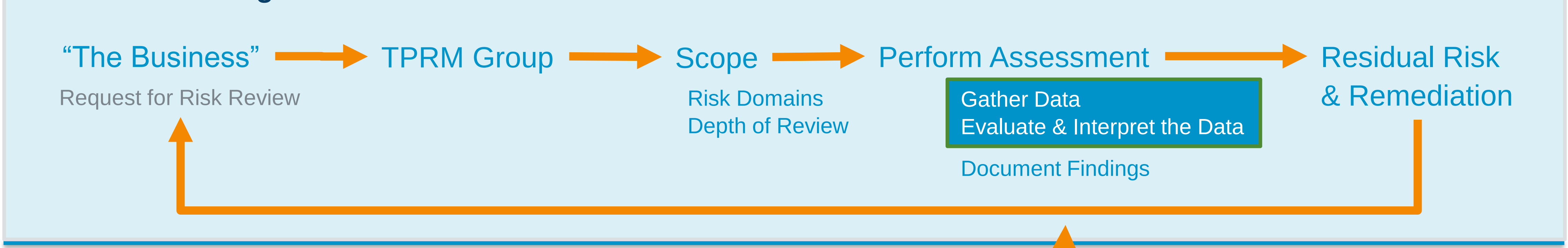
High

Medium

Low

Risk Domains & Review Depth

- IT (Information Security, Cyber)
- Non-IT (Compliance, Financial, Geographic, Identity)



Your TPRM Program

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

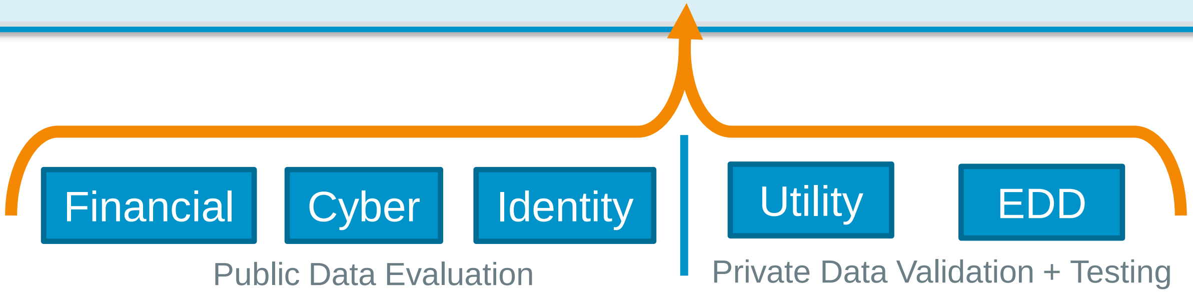
"The Business": Request for Risk Review

Scope: Risk Domains, Depth of Review

Perform Assessment: Gather Data, Evaluate & Interpret the Data, Document Findings

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



Financial | Cyber | Identity — Public Data Evaluation

Utility | EDD — Private Data Validation + Testing

ProcessUnity

Summary: Rationalize Your Due Diligence

Categorize & Risk Map the Products/Services You Use

Planning using triggers for the types of risk to monitor and the threats that are presented based on the nature of the third-party relationship can reduce cycle times while ensuring the right due diligence is performed at the right level.

Leverage External Data Where/When it Makes Sense

Public Data – Intelligent data (BitSight, RiskRecon, Refinitiv, D&B etc.) augments your teams' assessments and creates an applied risk view of your vendor population. **Private Data** - Utilities / Exchanges are a piece of the puzzle. Outsourcing specific tasks / portions of the process can enable scale.

Embed Your Risk Process Into the Onboarding Cycle

Auto-scoping and review saves time and reduces vendor fatigue, auto-scoring ensures accuracy and consistency. Reducing busy work = more time for strategic risk management and cost savings.

Consider All Aspects of a Vendor's Risk Profile

Identity, Financial, Reputation, Cyber, Resiliency, Privacy, Compliance, Geographic, Fourth-Party, Conflict of Interest, etc.

Remember: You will always own the risk!

Your internal process/program must ultimately determine acceptable risk levels – combining internal and external data gives the most accurate picture of risk.

ProcessUnity Vendor Intelligence Suite

Vendor Cyber Intelligence

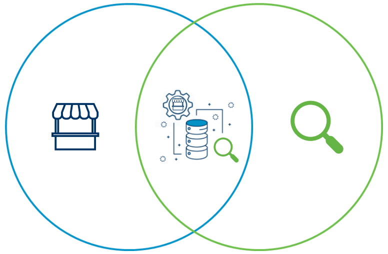
BITSIGHT
The Standard in SECURITY RATINGS

Onboarding Insights

Vendor Financial Intelligence

Integrated Assessments

Vendor Screening Intelligence



Continuous Analysis

Best Practices…*fully integrated and configured!*

Vendor Cyber Intelligence with BitSight

ProcessUnity
TPRM Program

BitSight
Cyber Screening

Intelligent Onboarding

Enhanced Due Diligence

Integrated Assessments

Real-time Issue Management

Continuous Cyber-analysis

ProcessUnity Vendor Cyber Intelligence with BitSight

Intelligent Onboarding

1. More informed third-party managers from understanding cybersecurity ratings
2. More comprehensive view of third-party's security posture
3. Reduced onboarding time through integration into due diligence

Enhanced Due Diligence

1. 350+ risk vector mappings to 80+ SIG questions = posture mapping on a per-questionnaire basis
2. Reduced analyst review time and more informed analyst reviews
3. Resulting ratings provide validation and high-quality data for analysis and will aid in key decision-making processes

Continuous / Ongoing Monitoring / Cyber Analysis

1. Reduced third-party risk mid-review cycle
2. Near-real time updates for proactive risk management
3. Reduced TPRM time in tracking and remediating issues

ProcessUnity

ProcessUnity Vendor Cyber Intelligence with BitSight

Integrated Assessments

1. Better assessment/questionnaire response evaluation via automated intelligence report
2. Cyber risk vector mapping eases assessment analysis and reduces time
3. Ratings improve validation and increase data quality to aid in key decision-making processes

Real-time Issue Management

1. Reduces the time third-party risk managers take in tracking and remediating issues
2. Reduces the time to create issues
3. Systematizes the issue creation process and reduces subjectivity

Dashboard

1. Vendor Cyber Intelligence dashboard provides a wholistic view of all the data within the third-party risk management program by focusing attention on all third parties being monitored by BitSight

For More Information

ProcessUnity

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 David Klein

david.klein@processunity.com

BITSIGHT

BitSight

www.bitsight.com

Contact Us

www.bitsight.com/contact-us

Blog

www.bitsight.com/blog

Contact Leslie Sloan

leslie.sloan@bitsighttech.com