Moving Beyond Traditional Suppliers

Presented by:
- Stacey Custeau – AVP, Third Party Risk
- Toby Downs – Sr. Third Party Risk Consultant

- ❑ Introduction
  - TPRM Program at Unum
  - Supplier vs Third Party
  - Program Maturity
- ❑ Identified Gap – 'Other Third Parties'
- ❑ Operating Model Concept
  - Documentation
  - Compensating Controls
  - Potential Pain Points
- ❑ Keys to Success
- ❑ Continued Evolution

Helping the working world thrive throughout life's moments™

Unum at a glance

39 million
people protected worldwide

182,000
businesses in the U.S. and the U.K. offer benefits provided by Unum

$7.5 billion
in benefits paid

#266
on the Fortune 500 list

1 in 3
companies on the Fortune 500 offer Unum benefits to their employees

4.7 out of 5 stars
97% reviewers recommend our products

Modern Financial Protections

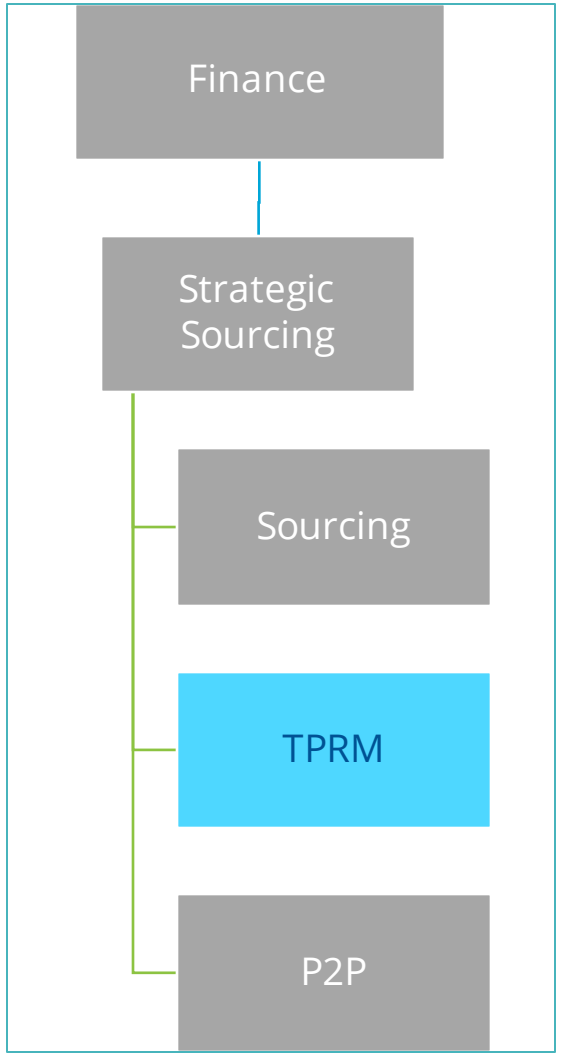
- Disability
- Life
- Stop Loss
- Accident
- Critical Illness
- Hospital
- Dental
- Vision

Innovative Leave Solutions

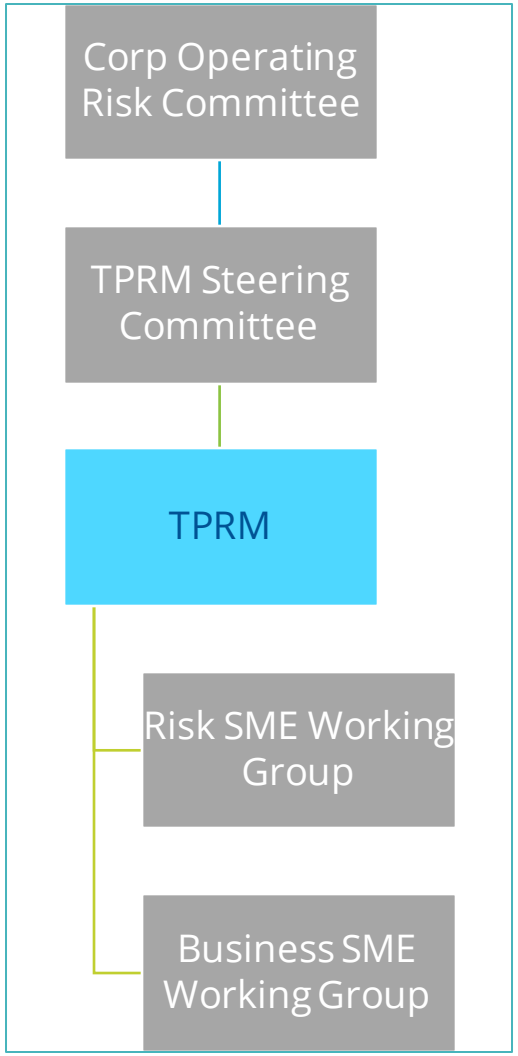
- Advanced absence management for employers
- Better leave experiences for employees
- Streamlined compliance processes
- Up-to-date data for insights and integration

Source: Unum.com/about

Reporting Structure



Governance Structure



TPRM Team - Key Accountabilities

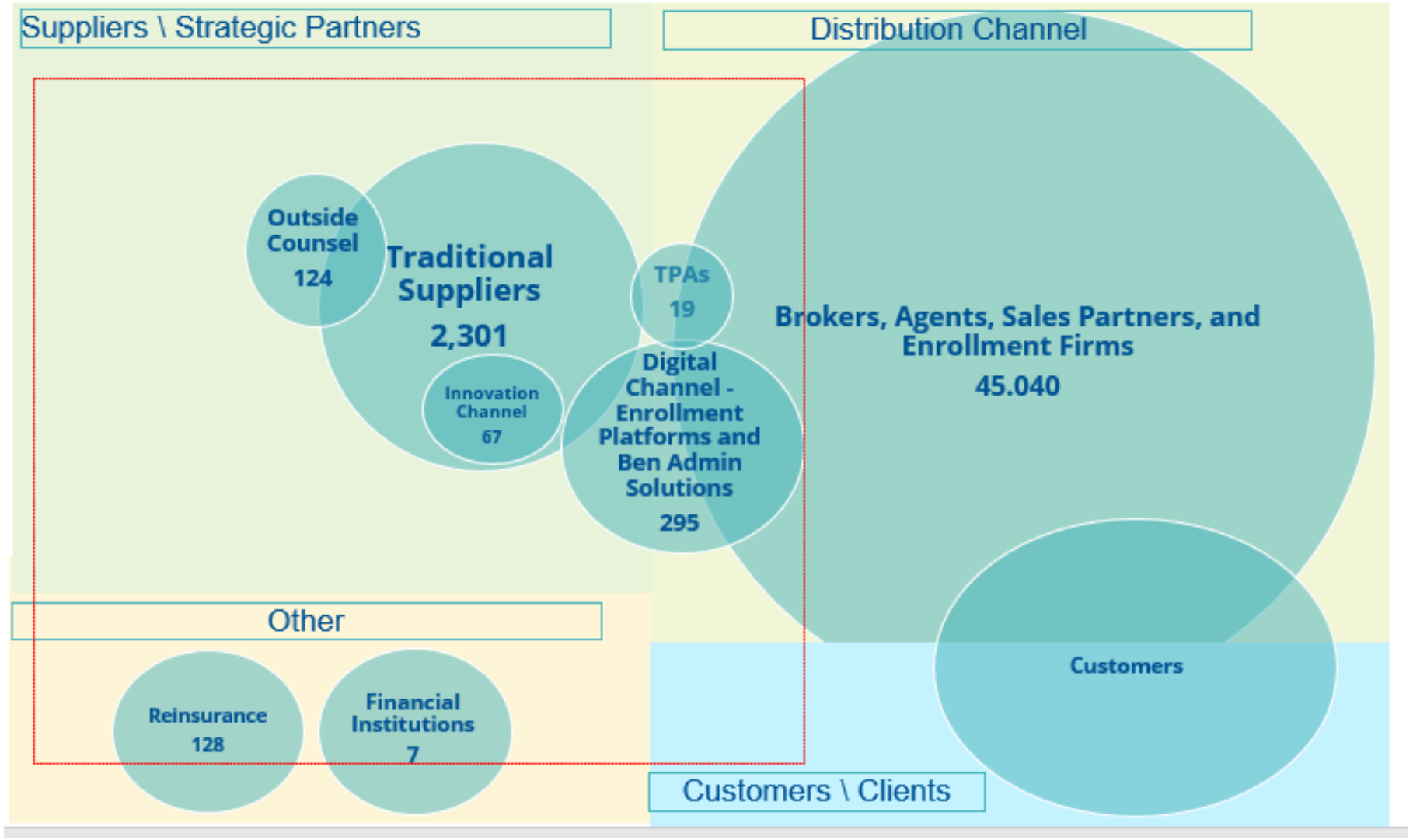
- Accountable for overall TPRM Program
- All third party onboarding via TPRM
  - Review all new engagements
  - Determine due diligence requirements for new suppliers and\or engagements
  - Own third party master file
- Create and maintain Foreign Locations playbook
- Manage ongoing Monitoring
  - Reassessment process
  - Issues Management
  - External Monitoring
- Own / maintain TPRM Platform

Defining / Finding Initial Inventory

Sources:

Accounts Payable data
General Ledger data
- Wire payments
- P-Card
- Commissions

Business areas
Legal
Audit
Compliance
Sourcing



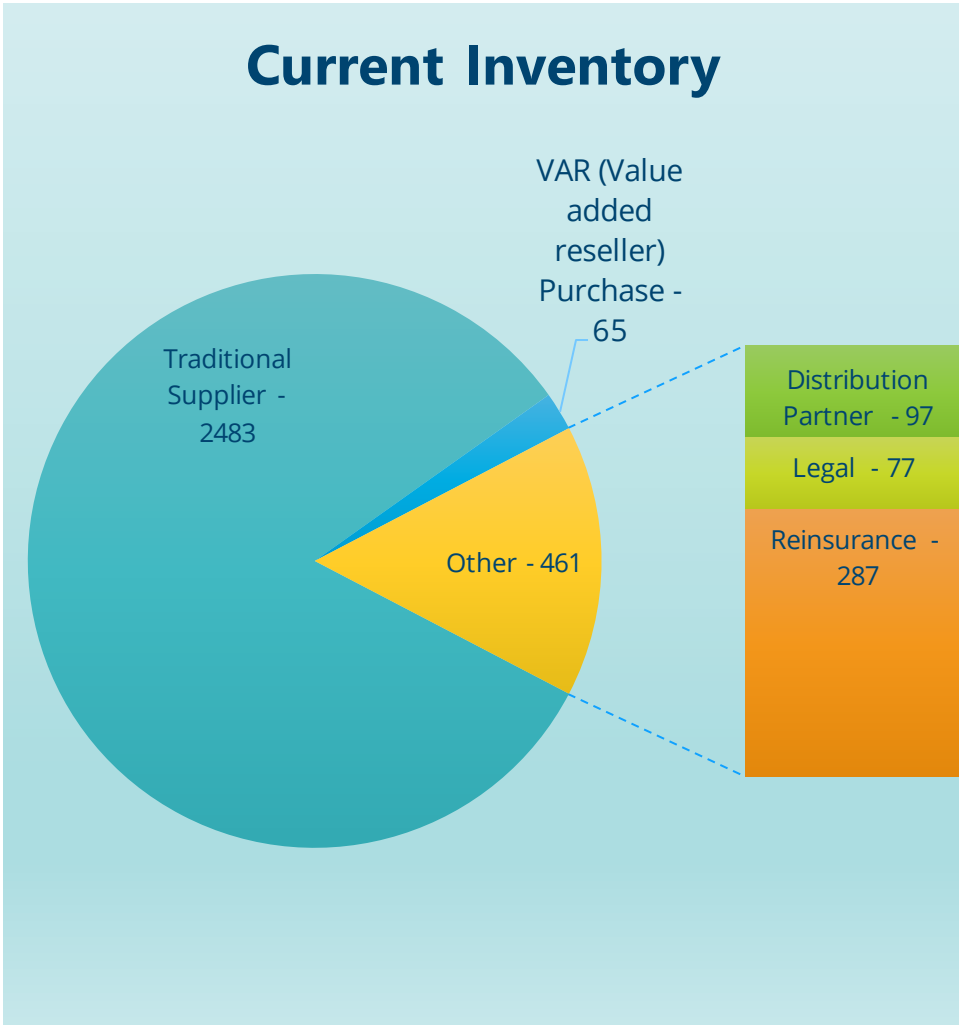
THIRD PARTY VS SUPPLIER

Third Party: refers to an unaffiliated entity (other than a customer) providing services in accordance with a defined business agreement with Unum.

Supplier: a subset of Unum's third party population that provides goods or services directly to Unum and is managed as part of Unum's supply chain.

WAYS WE DIFFERENTIATED:

- Are they paid via invoicing process?
- Do they have contracts?
- Who facilitates the 'contract'?
- Does the Sourcing policy apply ?
- Is there increased oversight or unique due diligence?
- Does the category pose an increased or decreased risk?



While all suppliers can be considered third parties, not all third parties are suppliers!

TPRM Program Evolution

2016

Supplier Risk Management Program established - Focus – Traditional suppliers

Implemented Optiv

1 FTE

2018

Hired Director – Third Party Risk – Focus on non-traditional third parties

Hired Supplier Risk Manager

2019

Audit Report – Identified gaps to 'Other Third Parties

Hired Third Party Risk Manager

Created first Operating Model – Digital Distribution Partners

Implemented Aravo

2020

Consolidated Supplier and Third Party – rebranded to TPRM

Created Reinsurance Operating Model

Enabled External Monitoring

2021/2022

Hired Data Specialist

Created Legal Operating Model

Expanded Distribution Operating Model to include all Distribution Partners

2023

Created Data Analyst Role – hired Data Specialist

Created new TPRM role in UK Office – Head of Sourcing & TPRM

5 FTE's

What problem(s) were we trying to solve?

Comprehensive Inventory

- Aggregate Risk Exposure
- Reporting
- Speed of response

Stakeholder Compliance

- Central entry point – Gate check
- Address Internal Audit action items

External Inquiry

- Respond to customer questions
- Regulatory Inquiries

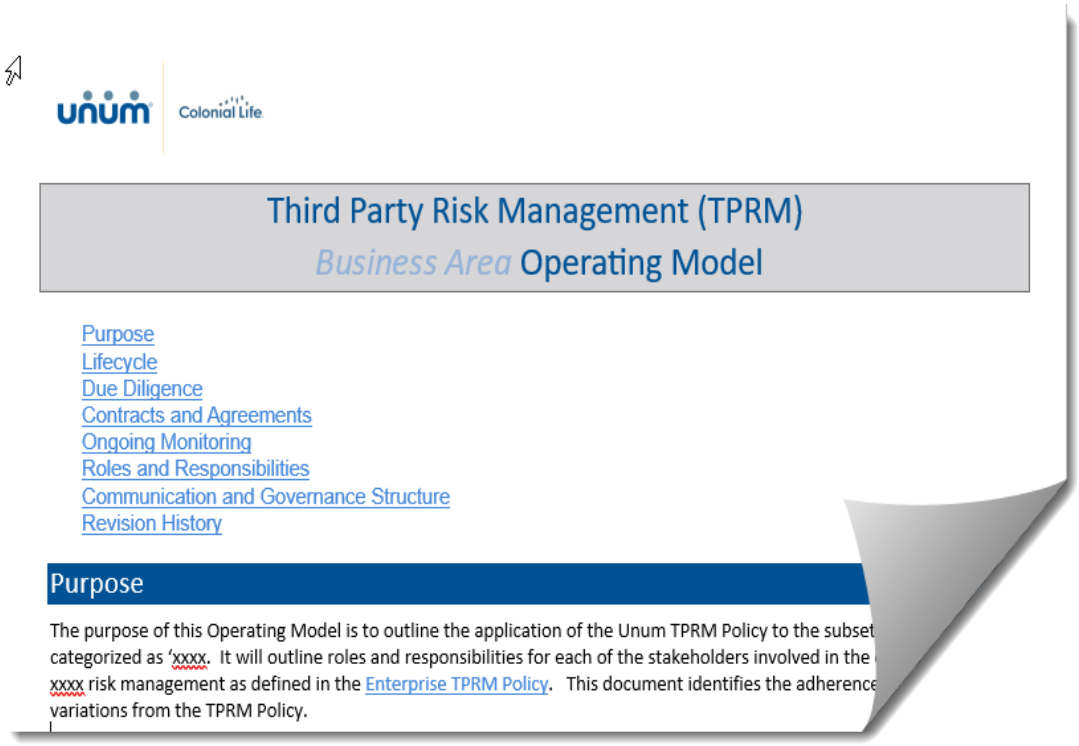
External Guidance

- Program consistency
- Brokers as TPSP

TPRM Operating Models

WHAT ARE THEY?

- **RISK BASED APPROACH** for Non-Supplier Third Parties
- Aligns to defined Third Party Risk Management Lifecycle
- Includes **clear roles and responsibilities** for stakeholders involved
- Identifies and leverages current **Controls and Processes** for category / sub-category
- Criteria Identified / Defined by **Business Stakeholder** with TPRM guidance
- Level of **due diligence** and TPRM support for **ongoing monitoring** defined in Operating Model in accordance with TPRM Policy
- VP or Higher **Ownership**



unum Colonial Life

Third Party Risk Management (TPRM)

Business Area Operating Model

Purpose

The purpose of this Operating Model is to outline the application of the Unum TPRM Policy to the subset categorized as 'xxxx. It will outline roles and responsibilities for each of the stakeholders involved in the xxxx risk management as defined in the Enterprise TPRM Policy. This document identifies the adherence variations from the TPRM Policy.

1) Use your existing lifecycle as a starting point
   - Identify what must stay the same (i.e. TIN Match / OFAC check)
   - Identify unique controls
2) Definitions
3) Roles & Responsibilities
4) Document variations at each stage
5) Communication / Governance

Lifecycle

The Enterprise TPRM Policy prescribes that there must be a proactive risk management effort throughout the entire Third Party Lifecycle, and that it is the business stakeholder's responsibility to ensure each stage is performed (either directly or with the support of the Third Party Risk Management Team and/or Corporate Functional Area). Further, the policy states that for each Third Party relationship, the five framework elements must exist.

Application of the Enterprise TPRM Policy to Unum Outside Legal Counsel includes the following in these lifecycle stages:

1. Planning and Initiation	2. Due Diligence	3. Contracts & Agreements	4. Ongoing Monitoring	5. Termination
•Understand Legal & Regulatory limitations of data sharing and usage	•Onboarding New Law firms •Completion of an Inheret Risk Assessments •Identification of Outside Legal Counsel that meets the criteria outlined in this Operating Model	•Ensure Engagement Letters or Services Agreements accurately reflects scope	•Financial Monitoring of Key Outside Legal Counsel •Re-assessment based on risk profile •Annual mailing of Protection Security Controls for Outside Counsel'	•Develop contingency plans for 'key engagements' •Ensure any Unum data is returned or destroyed – Submit 'Certificate of Destruction' to TPRM@Unum.com

Potential Compensating Controls

Dedicated Relationship Management Teams including Full-Time Relationship Directors

Annual Review (minimum) of Relationship(s) including metrics, performance, delivery

Quarterly Business Stakeholder Working Group

Annual Proactive Communication of Information Protection and Security Controls

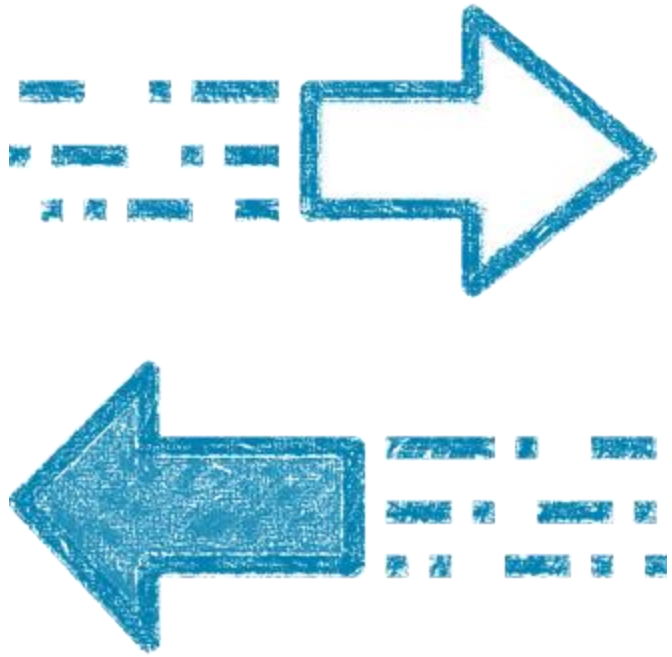
Scheduled (and unscheduled) touchpoints with TPRM

For Discussion: What are some others?

Potential Pain Points

- **Contract Language / Appetite to Change Third Parties**
  - Legacy contracts may not contain due-diligence / explicit right-to-audit obligations – risk of 're-papering'
  - Lack of appetite on part of stakeholder to stop doing business

- **Who really owns the Data?**
  - Direction of the data
  - Who took custody of the data from the customer
  - How is it used? Is it enriched?



- **Program Maturity**
  - Position as value prop for our mutual customers
  - We both want to do the RIGHT THING (protect our customer's data)
  - Finally (and LAST) remind them of Regulatory Reasons
    - NYDFS (23 NYCRR 500.11)
    - NAIC Insurance Data Security Model Law
    - Federal (HIPAA, Interagency Guidance, SEC)

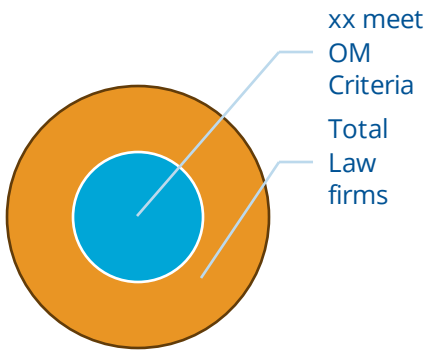
Operating Models are not "One-and-Done"!

	Operating Model Version	Reason for Update
Distribution	• 3/2020 – Initial Release • 10/2022 – Update / Expansion of Categories	➢ Audit Findings ➢ Corporate Risk Focus, Business Area Updates, Regulatory Changes
Reinsurance	• 7/2021 – Initial Release • 7/2022 – Update / Definitions • 2024 (upcoming)	➢ TPRM Initiated ➢ Test & Learn ➢ Corporate Risk Focus
Legal	• 7/2021 – Initial Release • 10/2023 – Update / Definitions, Risk Tier	➢ TPRM Initiated ➢ Test & Learn, TPRM Program Maturity

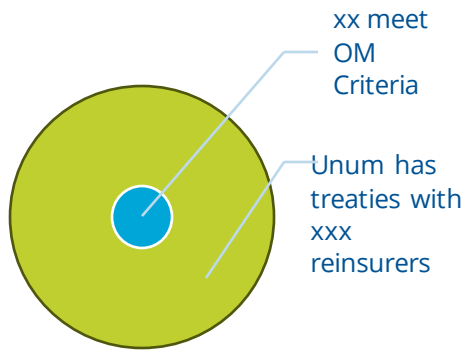
SOME REASONS FOR CHANGES

- TPRM Program Maturity
- Regulatory Changes
- Business Area Updates
- Corporate Risk Focus
- Test & Learn!

Legal



Reinsurance



Keys to Success / Helpful Hints

- ✓ Ensure you differentiate in your inventory
- ✓ Proactive Audit Review of concept
- ✓ Socialize with Senior Leaders of business area prior to building
- ✓ Focus on what is different from your 'standard' process
- ✓ Let the business help you define (shared ownership)
- ✓ Seek input from other risk SME's
- ✓ Be prepared to spend more TPRM time on non-traditional third parties
- ✓ Document, Document, Document

Increasing our Due Diligence

CURRENT STATE:

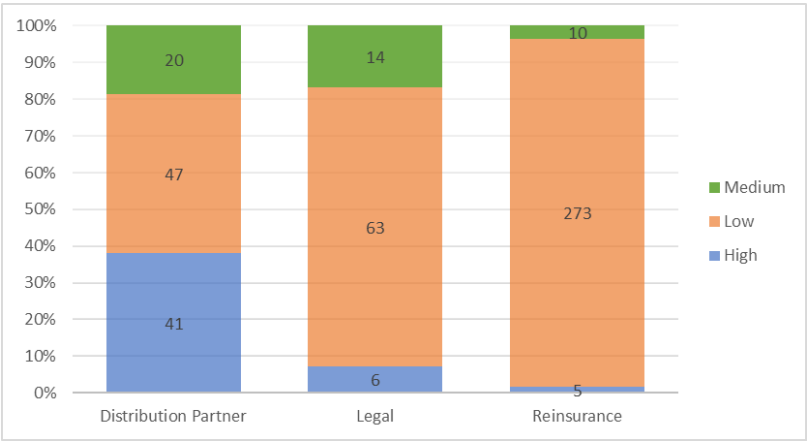
- Medium Risk Third Parties covered by an Operating Model (Distribution, Outside Legal, Reinsurance), current due diligence limited to an "initial survey", primarily focused on locations, regulations, and connection mechanism (if applicable) – no questions related to existing controls. Continuous Monitoring if Data/Connection.

PROPOSAL

- Adopt "Compliance Questionnaire" based on the LICONY Third Party Service Provider Due Diligence Questionnaire (17 questions).
  - Medium Risk Third Parties covered by an Operating Model (Distribution, Outside Legal, Reinsurance) (not limited to NY)

ACTIVITY TO DATE:

- Jan 2023 – Socialized W/Operating Model Owners
- Oct 2023 – Presented concept to Working Groups & TPRM SteerCo
- Jan 2024 – Updated draft from Privacy/Compliance:
- Jan/Feb 2024 - Scoping & draft build in Aravo



For Discussion:

What if they answer "No"?

- *Define remediation*
- *Escalation Process*
- *Reporting*
- *Non-Conformant status*
- *Other*