



Third Party Risk Management

**Industry Current State
For Discussion**

September 12th, 2018



Summary

- > Context
- > Overview
- > Current State Understanding
 - TPRM Governance & Oversight
 - TPRM Lifecycle
 - TPRM Enablers
- > Market Maturity
- > Next steps

Context



Privacy practices will be the next consumer-driven, value-based source of differentiation

54% of consumers... like to buy products that are environmentally friendly

You face many conflicting priorities

Do customers care about what you do?

- › Protect customers from **risk**
- › **Co-innovation** with suppliers
- › **Enable** colleagues to buy what they need quickly and easily
- › You need **modern, smart, flexible software**



Customers care who you pick as suppliers...

- Safe & Secure
- Reliable
- Ethical

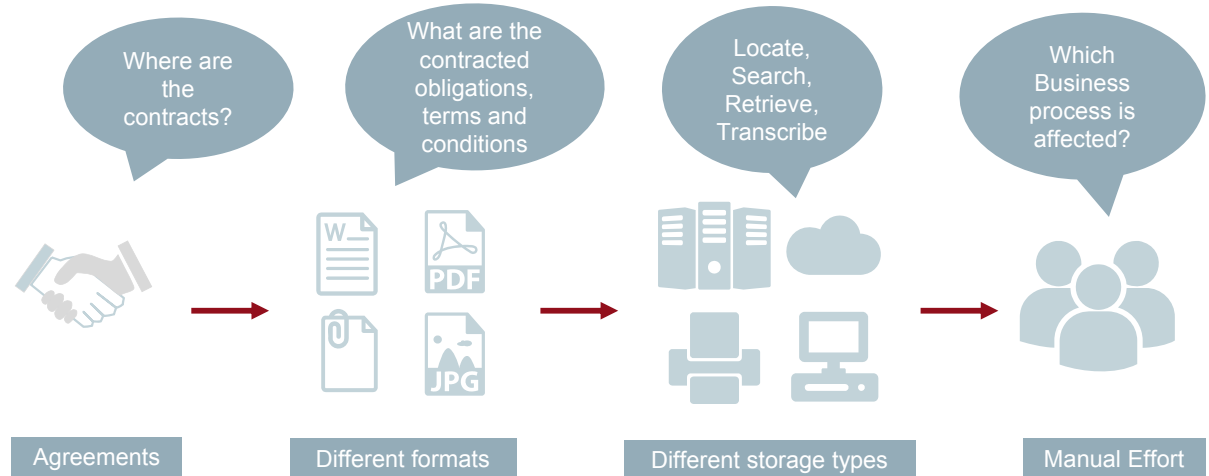
Source: Forrester Data Global Business Technographics Priorities & Journey Survey, 2018
Technology purchase influencers



Industry Insights

Document Management Challenges

Today's challenges:



47% of firms use spreadsheets to track issues and only 12% of firms feel their risk management tools are well integrated into their overall risk management reporting systems
– EY TPRM survey

Global Insights into Third Party Risk Management

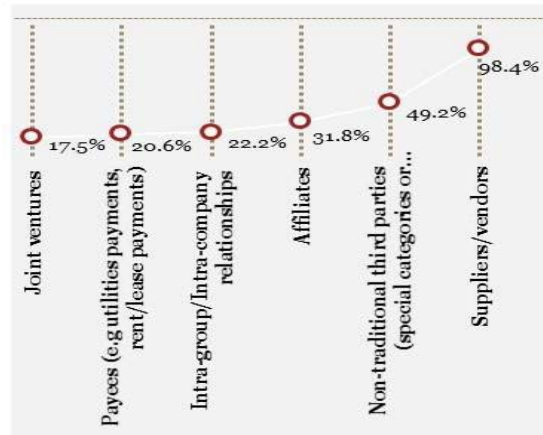
Recent *Third Party Risk Management* survey has also revealed that a growing number of financial institutions are relying on technology to enable their TPRM programs, however response times for key reporting continues to be a challenge:

TPRM and Cyber Security

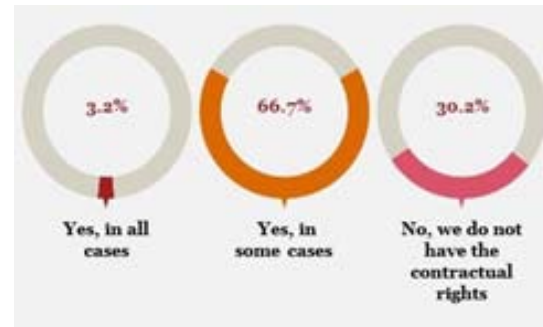
A number of recent cyber security incidents linked to 3rd or 4th parties highlight the need for a strong Enterprise-wide TPRM program:

- **Sears, Delta Airlines and Best Buy, 2018** – data breach occurred through a common third party providing services related to online chat, virtual agent, etc. allowing them to access payment information
- **Google, 2017** – the third party of one of the travel providers used by Google (i.e. fourth party) was breached leading to cyber attackers entering the network and accessing Google employee information
- **Verizon, 2017** – the business partner of Verizon who facilitates customer service calls had used a third party to provide web services support (i.e. fourth party to Verizon). Cyber attackers had entered through the fourth party gateway and ultimately obtained access to millions of records of Verizon customer data.

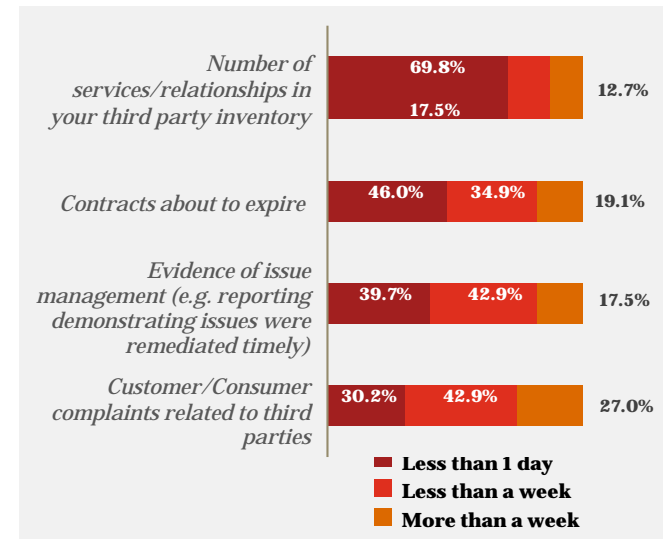
Scope of organization's TPRM program?



Contractual rights to perform due diligence or monitoring on 4th parties?



How quickly would your organization be able to report on the following?



Source: PwC: *Third Party Risk Management Survey Highlights*
Financial Services
March 2017

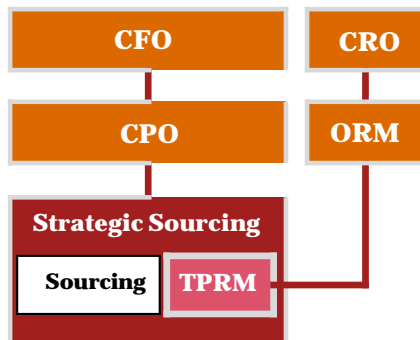


TRPM Program Organizational Alignment

The TRPM functions organizational alignment is one of the most challenging decisions faced by many institutions. Outlined below are the three common reporting relationships we have observed across the financial services industry.

Industry Observed Model 1

TPRM direct report to CPO with dotted line reporting to ORM

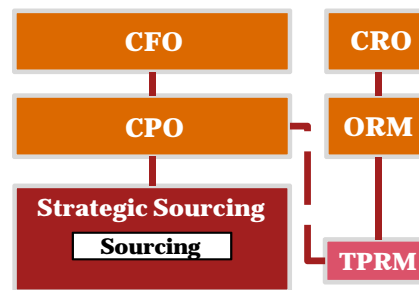


Key Highlights

A direct reporting line to a Sourcing function can help a TPRM function stay close to the business and become integrated into an organization's overall sourcing lifecycle. However, the 1st line alignment of this model can create difficulties in demonstrating the third party risk related independent challenge, which would need to be executed by ORM.

Industry Observed Model 2

TPRM function is bifurcated from Strategic Sourcing and reports to ORM and eventually the Chief Risk Officer (CRO)

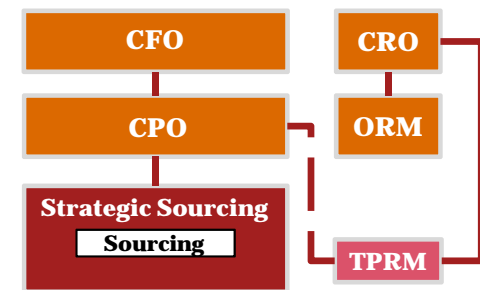


Key Highlights

A direct reporting line into ORM establishes TPRM as an independent 2nd line of defense function. This reporting structure enables the TPRM function independently challenge the 1st line of defense, however TPRM related activity execution is placed more squarely on the Sourcing function and the Business, without the benefit of a first line embedded TPRM function.

Industry Observed Model 3

TPRM function is bifurcated from Strategic Sourcing and reports to the Chief Risk Officer (CRO)



Key Highlights

A direct reporting line into the CRO establishes TPRM as an independent 2nd line of defense function. Similar to model 2, this model enables the TPRM function to independently challenge the 1st line of defense, and in some organizations, elevates the TPRM function's stature through its direct reporting line to the Chief Risk Officer.



Overview

Industry Trends



Robotic Process Automation (RPA)

- an automation based on defined rules
- can perform tasks involving different existing systems and applications
- adaptable to the size of the organization

example of application: self-assessment of third party risks, risk appetite profile, production of risk reports



RPA Cognitive

- Trend identification
- Predictive analysis
- Machine learning
- Unstructured data management

example of application: scenario analysis, analysis of operational losses



Artificial Intelligence (AI)

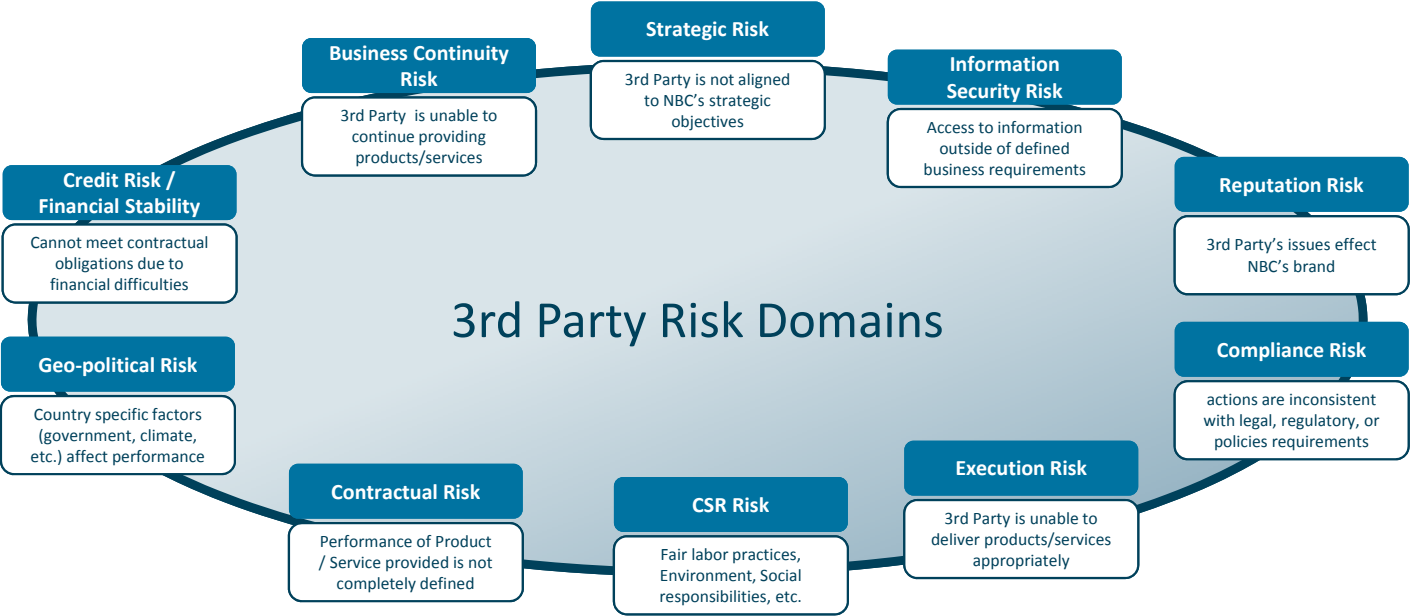
- Automation of decisions
- Optimization
- Anticipatory actions

example of application: scenario analysis and decision-making based on projections, analysis of risk assessments, loss analysis and anticipation of operational incidents



Proactive risk management and oversight is an imperative

Third party risk is a combination of other risks with various degrees of severity based on the maturity of the relationship with the third party. The potential risk exposure from doing business with third parties goes well beyond direct financial loss and includes reputational damage, regulatory scrutiny and customer attrition.



The 3rd Party Risk Domains listed above also apply to 4th parties (sub-contractors) as an extension of 3rd party risks

source: Industry Experts

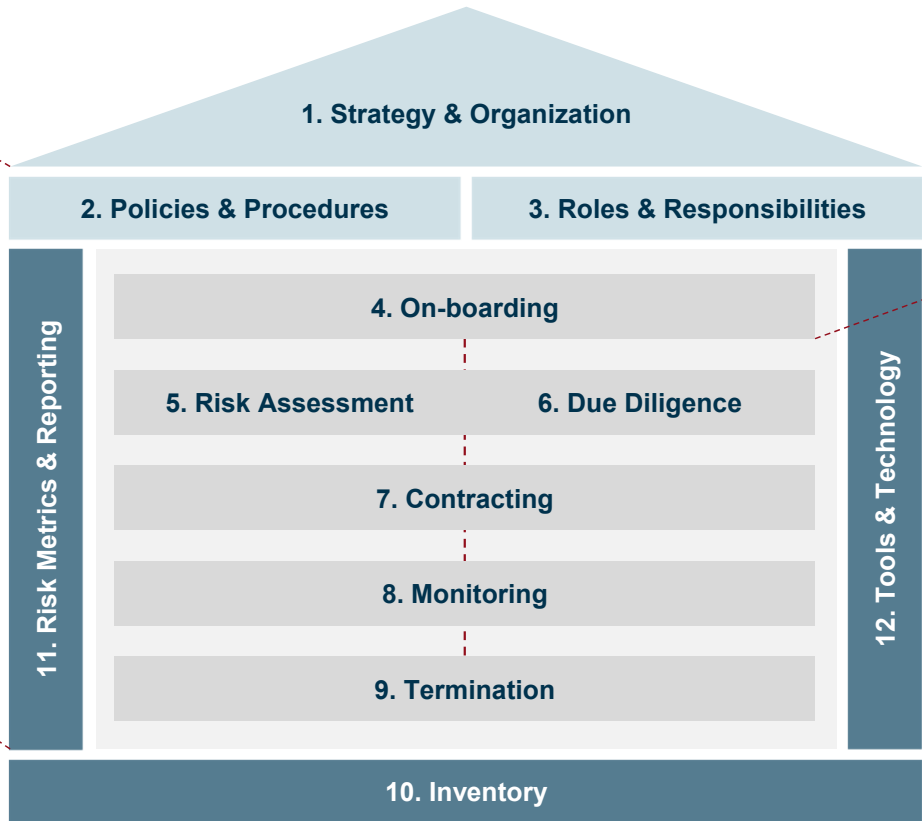
Overview TPRM

Governance & Oversight

The organizational structure, committees, and roles and responsibilities for managing third parties.

Enablers

Support third-party management processes.



Lifecycle

The process to manage risks across the third-party lifecycle:



Focus on 3rd party risks to meet business requirements

- ❑ Business opportunity to capture 3rd party⁽¹⁾ management **value** (savings, avoided costs and uncounted gains such as acquisition of high-level expertise, talents, agility in peak periods, modernization of processes, mitigation of risks, customer satisfaction, etc.);
- ❑ Increased dependencies on our 3rd parties to deliver the **client promise**;
- ❑ Rapid changes in business landscape⁽²⁾ requires a formalized proactive risk management and oversight to lessens probability of business disruption;
- ❑ Strong recommendation from regulators to implement a formal framework and oversight pressures worldwide to add controls for 3PRM;
- ❑ Major **cultural shift** is required for successful deployment of a robust framework.

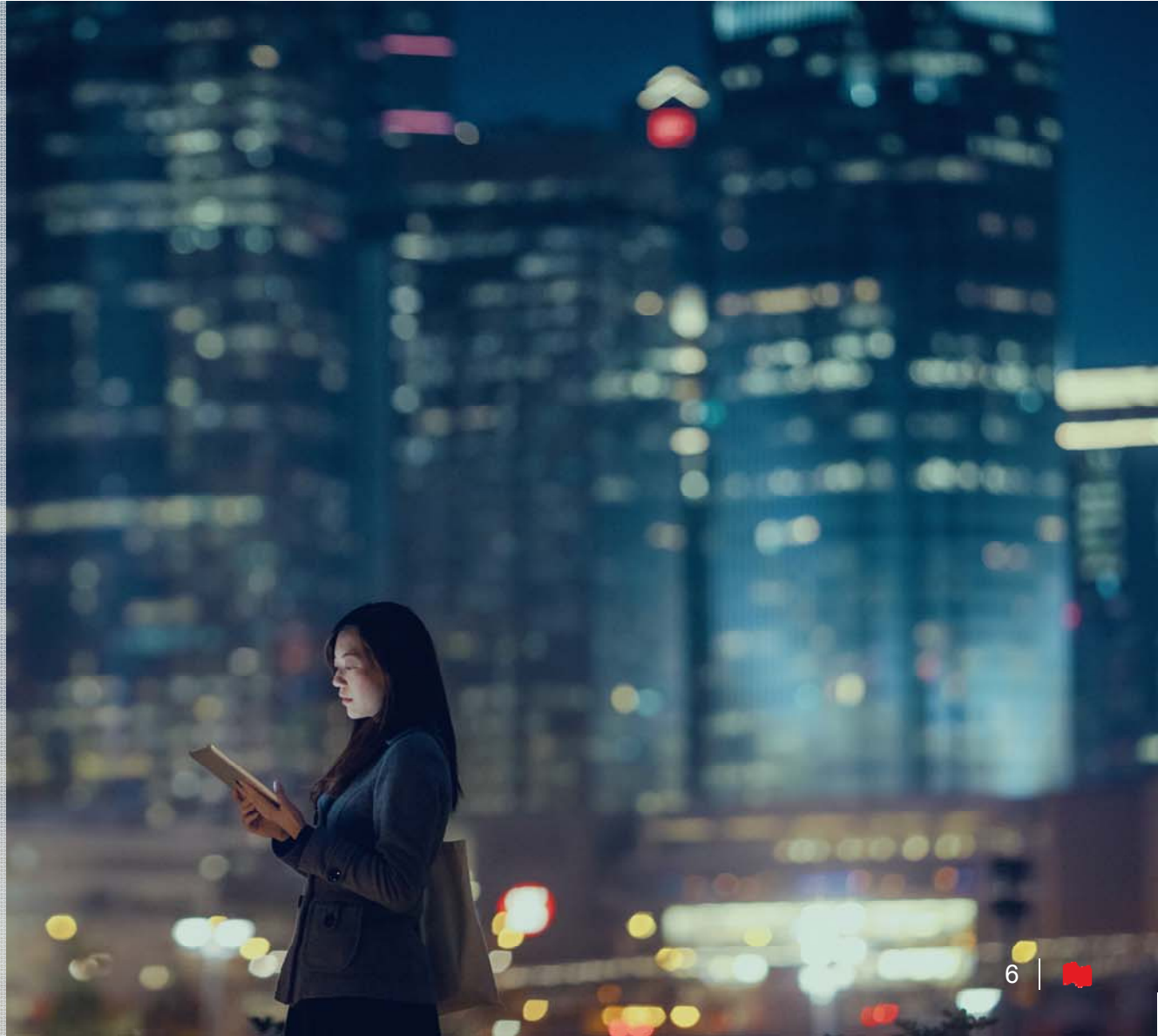
Failure to effectively manage 3rd party risks could potentially expose organizations to security/data breaches, service disruptions, regulatory penalties, financial loss, litigation or reputational damage

(1) Appendix A: 3rd Party Definition

(2) Appendix B: Emerging Industry Trends














Current State Understanding



Current State

Executive Summary

Topic	Industry Current State	Assessment
Strategy & Organization	The Strategy and Organization is generally aligned overall with regulators' expectations and industry peers, however the operating structure is not clearly defined nor understood by stakeholders.	
Policies & Procedures	Policies are generally aligned with regulators' expectations overall, however formal procedural documentation to define the roles, responsibilities, and expectations of stakeholders could be improved as well as a standardized process for communicating the policies and procedures.	
Roles & Responsibilities	Overall, the role of the Risk Management Committee is generally aligned with regulatory expectations, however procedures on the reporting and escalation process should be defined. High-level roles and responsibilities are defined, however, the roles defined in the RACI require updating and are not clearly outlined in the policy.	
Onboarding	Overall, the onboarding process is generally aligned with industry peers, however the process is not consistently followed by all business lines. There is still room to review and improve this process.	
Risk Assessments	The Risk Assessment process is generally aligned with regulators' expectations overall, however there is limited documentation. Most organizations are reviewing and improving this process to make it more efficient and simple.	
Due Diligence	Supporting documentation related to the due diligence review is not clearly defined and is not stored in a central location.	
Contracting	Overall, the contracting process is generally aligned with regulators' expectations and industry peers, however as per management, some agreements are signed before risk assessment and due diligence. Improvement of this process would reduce the risk level.	
Monitoring	The operating model related to the monitoring process and the issue management process (including escalation process, issue follow-up, etc.) are not fully designed.	
Termination	The Termination process is not formalized and/or standardized in the majority organizations.	
Inventory	Organizations do not currently have the proper tools and processes in place to centralize the 3 rd party inventory.	
Risk Metrics & Reporting	There is an opportunity to improve the reporting related to KPIs or KRIs. The process related to annual attestation is under review.	
Tools & Technology	The tools and technology currently used are not optimal. There is an opportunity to review and improve book of record for single source of truth.	

Legend:  Enhancement opportunity  Needs Improvement

Risk Based Approach

What?

- Improve 3rd party performance management
- Proactively manage risks (identify, take action and monitor)
- Balanced portfolio management



Unbiased review of issues...



Statistical Sampling



How?

- Smart data ingestion
- Complete data analysis
- Improved detection effectiveness



Finding issues rather than confirming their absence

Oversight & Governance

Principles of good governance & key model elements

Proactive 

Strong Governance Framework

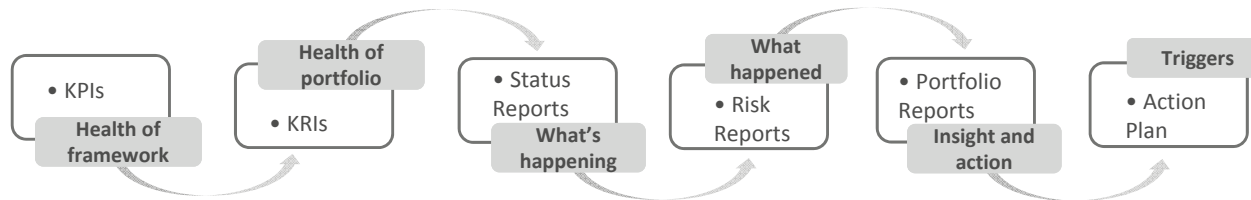


Key enabler allowing easy access to 360 view of 3rd party (KYV)

Convenient 

Accessible 

E2E view of mgmt process



Key Enablers

Analytics & Actionable Reporting

Defined Risk Appetite Statement and KRIs

Based on strategy and business practices, a *risk appetite* should be targeted in recognition of 3rd party risks inherent for each LOB models.

Centralized Data Integrity and Analytics

Clearly defined risk based frameworks exist to determine the re-assessment frequency of 3rd party. Elements of residual risk are used to determine the frequency of assessments to perform.

Systematic solution used to store files and data; process or work flow fully enabled by technology and continually assessed for efficiency and alignment with the process.

Supplier Information & Performance Management (SIPM)

SIPM is the enterprise tool to identify, assess, manage and monitor 3rd party risk throughout the partnership lifecycle

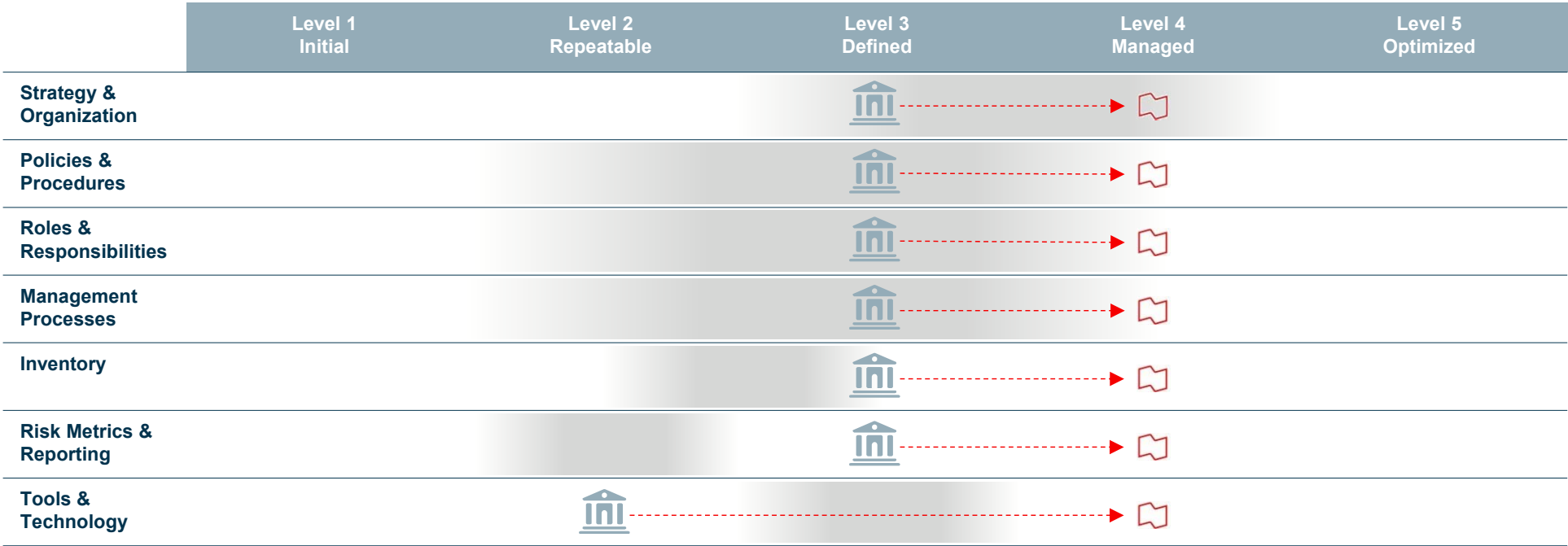


Workflow • Central Repository for pre-defined artifacts • Notifications
• Track open items • Reporting • Analysis • Change Management

Maturity Assessment



NBC TPRM Program Maturity Progression



Industry Peers
 Minimum Requirements

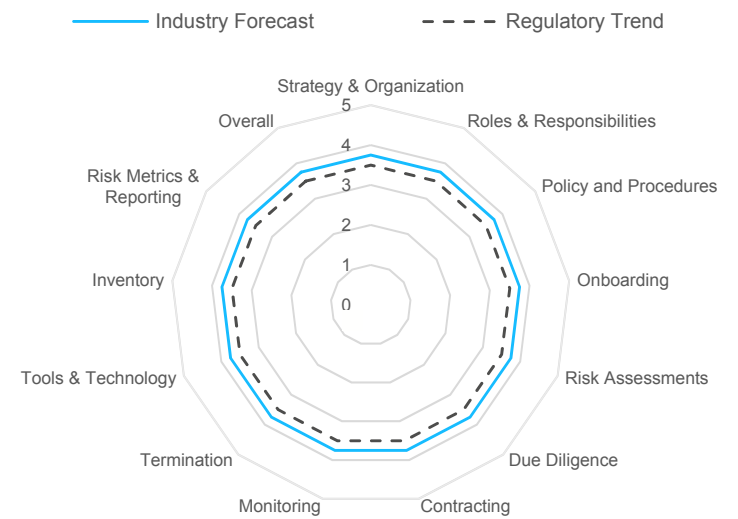
 Future State

TPRM Program Current vs. Future State

Today



Tomorrow



Most organizations are keeping up with industry peers overall, but not meeting key regulatory requirements.



An organization should take charge of TPRM to position itself ahead of emerging regulatory and industry trends.

Executive Summary

Organizations will be **leveraging technology** to energize 3rd party relationship management by:

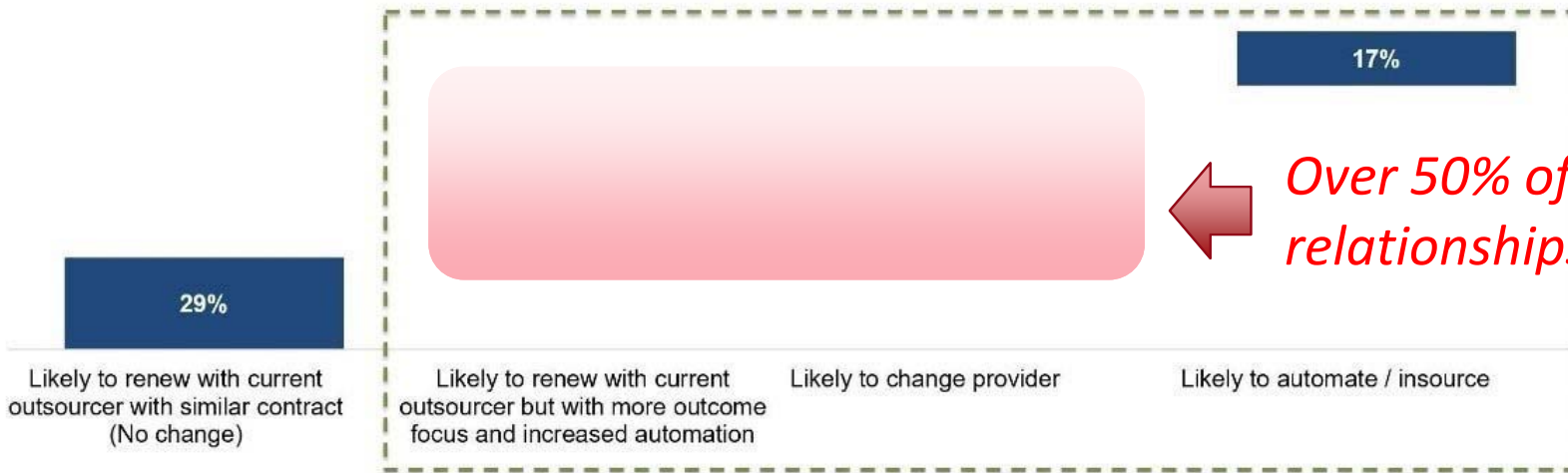
- Giving relationship management a strategic role in driving improved trust, alignment and collaboration between an organization and the 3rd party.
- Accelerating **transition** to a scientific, **data-driven management** of strategic 3rd party relationships leveraging automation and **advanced analytics**. This approach makes the relationship management process more measurable and objective.
- Driving **improved results** in strategic 3rd party engagements through technology-driven relationship management strategy.

Industry Insights

Opportunities to growth market share

Only ~30% current outsourcing contracts are safe!

What are your plans regarding current outsourcing / managed services agreements you have?



Over 50% of business relationships can be secured...

~70% outsourcing clients are expected to change their outsourcing relationships in some shape or form

Source: HfS Research in Conjunction with KPMG, "State of Operations and Outsourcing, May 2018
Sample: Enterprise Operations Leads = 381



NEXT STEPS

- > **Validate current state with regulatory requirements (your organizations or clients)**
- > **Plan workshops with key stakeholders and prioritize according to gaps**
 - **Risks identification and assessments**
 - **Actions required to mitigate**
 - **Monitoring and report to senior management**





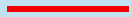
LET'S KEEP GOING!

*“Those who are crazy enough
to think they can change the world
usually do.”*

Steve Jobs



APPENDIX



3rd Party Definition (Appendix A)

How 3rd parties are defined	General definition	An entity, including individuals and affiliates, that has a business relationship with the institution or its customers, and is not itself a customer. Third party relationships include:
	Vendor 3rd Party	'Vendor' third party are service providers that deliver a product or service to the institution. These relationships are typically sourced through a sourcing / procurement process. Payment is typically transacted by Accounts Payable.
	Non- Vendor 3rd Party	'Non-Vendor' third party relationships are typically acquired by a business line / segment directly, not through a sourcing / procurement function. Financial remuneration, if applicable is typically transacted outside of Accounts Payable processes. These relationships may be managed solely by a business line / segment, or managed in conjunction with a corporate risk management function.

CATEGORIES (Non-Vendor)	Specialized Analysts and Advisors	Counterparties
	Affiliates	Debt Underwriters / Securitization Firms / Trustees
	Affinity Relationships	Financial Utilities
	Alliances and Partnerships	Government Special Purpose Entity (GSE)
	Brokers	Indirect Lending
	Correspondent Banks and Wholesale Banking	Joint Marketing Partners
	Rating Agencies	Tenants
	Servicers	Trade Associations



Emerging Industry Trends (Appendix B)

As our procurement organization matures, the focus needs to be more than just cost savings; we need to be proactively involved in strategic initiatives and creatively protect the organization.

Procurement and Finance Alignment	<ul style="list-style-type: none">• Essential partnership between procurement and Finance (BU CFO) to track and record savings
New Risk Domains	<ul style="list-style-type: none">• Extension of 3rd Party Risk Management to address additional risks beyond Information Security and Supplier Performance (Reputation, Compliance, or Geo-political Risk)
Sub-Contractors (4th Party Risk)	<ul style="list-style-type: none">• Inclusion of Sub-Contractors in the Risk Management Program, including inventory, assessment and monitoring (Supply Chain Management)
Innovative Solutions	<ul style="list-style-type: none">• Expand supply market research to include new innovative solutions (i.e. Cloud, social media, etc.)
Revenue Optimization	<ul style="list-style-type: none">• Promote and develop the customer portfolio within our supplier community and maximize value to the organization by being thoughtful about our customer/supplier relationships
International Expansion	<ul style="list-style-type: none">• Support strategic initiatives in international expansion, licensing, e-Commerce growth
M&A / Divestitures	<ul style="list-style-type: none">• Ongoing M&A and Restructuring activities have created new sourcing leverage and required new supply strategies
Sustainability	<ul style="list-style-type: none">• Increasingly, customers and governments are demanding for plans to make operations more sustainable and from a more diverse supplier base

source: Industry Experts

