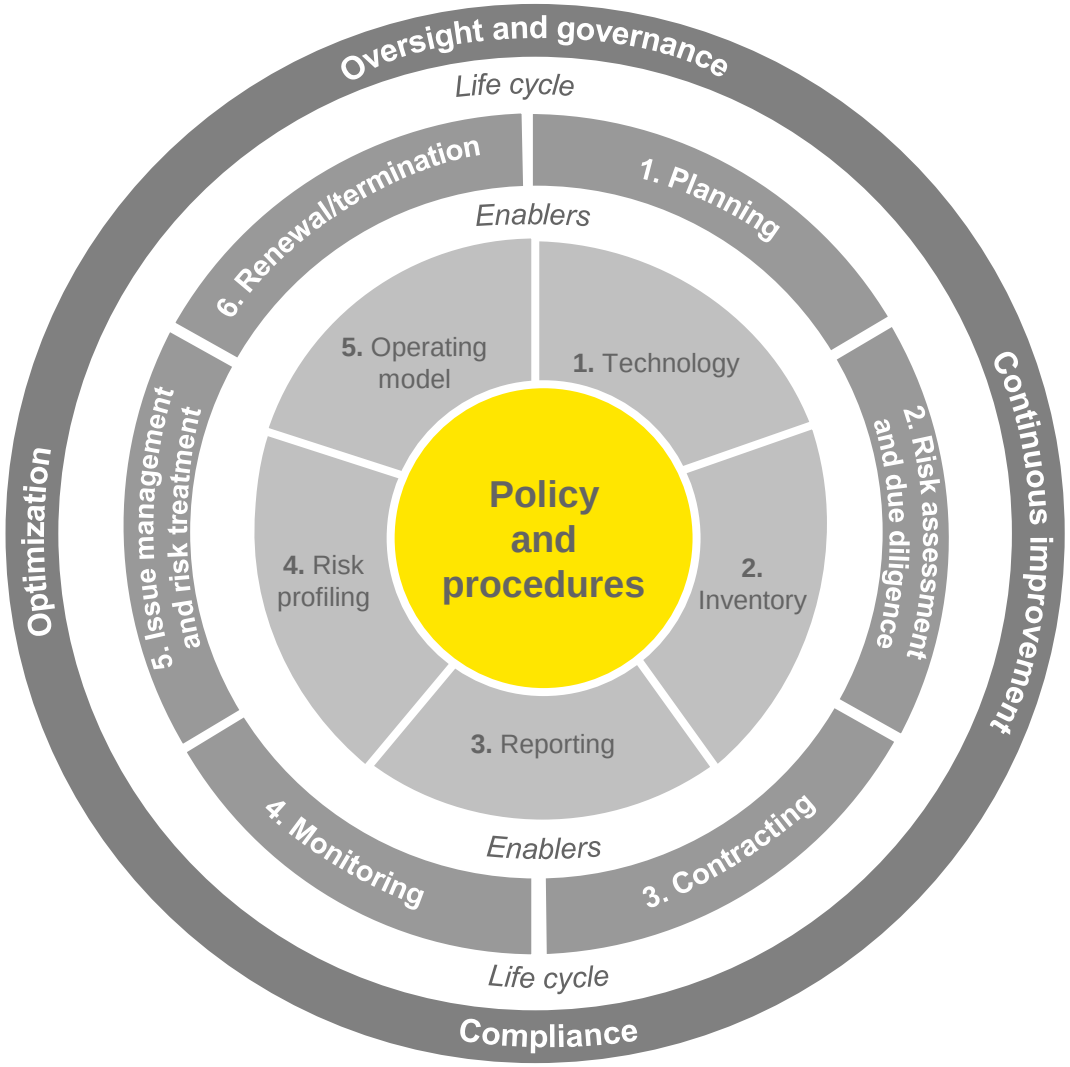
Third-party risk management (TPRM) – regulatory and industry trends

June 2018

Building a better working world

Contents

Section



Regulatory trends

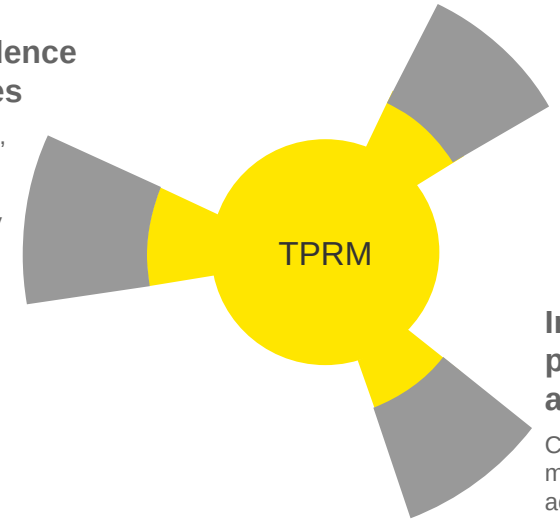
Third-party risk management

Third-party risk management provides a function for management to identify, evaluate, monitor and manage the risks associated with **third parties** and **contracts**.

Key drivers for third-party risk management

Extensive dependence on the third parties

Key operational, financial, compliance, and technology-related functions are increasingly placed in the hands of third parties.



No single ownership and inventory of third-party relationships

There is often not a single place of responsibility for broader third-party performance and risk management.

Increased data protection obligations and regulatory focus

Complex laws and regulations mandate that corporate control activities extend to third parties.

Benefits of TPRM

- **Risk mitigation and reduction**
  Third-party risk identification, development and implementation of appropriate risk management strategies, and establishment of ongoing monitoring
- **Increased efficiency**
  Eliminates overlapping and/or redundant TPRM practices, thus reducing the cost of managing risks
- **Governance of emerging third-party risk**
  Proactive identification and management of emerging risk indicators and regulatory requirements
- **Greater risk insights to drive performance**
  Risk governance that becomes forward-looking and can influence strategic decisions

Industry and regulatory themes for TPRM

Organizational model

- Developing more centralized organizational structures aligning to the three Lines of Defense Model (3LOD)

Cybersecurity

- Making sure policies and information procedures are designed to safeguard the security of systems and nonpublic information accessible to third parties
- Requiring third parties to meet minimum cybersecurity requirements

Assessment framework

- Considering the use of consortiums within many aspects of TPRM, specifically for common assessment framework
- Identifying and monitoring external parties beyond third parties (i.e. fourth, fifth, nth parties)

Evolving regulatory expectations

Increasing regulatory and industry focus on IT security/cyber and resilience/recovery and privacy in connection with third parties.

FDIC: FIL-44-2008: Guidance for Managing Third-Party Risk

CFPB Bulletin 2012-03 and 2012-07: Service Providers

FRB Bulletin SR 13-19/CA 13-21: Guidance on Managing Outsourcing Risk

OCC Bulletin 2013-29: Third-Party Relationships: Risk Management Guidance

SEC's National Exam Program (NEP) included IT security and Cyber as an examination priority; inclusive of Third Party oversight

FDIC, OCC and FRB: Advanced Notice of Proposed Rulemaking (ANPR) included enhanced cyber and resilience standards that apply to large financial institutions' third parties

European Parliament, Commission and the Council of the European Union (EU): General Data Protection Regulation (GDPR)

OCC 2018 publications: Fiscal Year 2018 Bank Supervision Operating Plan and OCC Semiannual Risk Perspective

2008 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 | 2018

FFIEC – Appendix J: Strengthening the Resilience of Outsourced Technology Services

NY DFS: Update on Cyber Security in the Banking Sector: Third Party Service Providers

FDIC revised Compliance Examination Manual: Section VII. Abusive Practices, including VII 4.1 – Third-Party Risk

OCC Bulletin 2017-7: Supplemental Examination Procedures for Risk Management of Third-Party Relationships

DOJ Evaluation of Corporate Compliance Programs

Key regulatory bodies:

- US Department of Justice (DOJ)
- Federal Financial Institutions Examination Council (FFIEC)*
- Office of the Comptroller of the Currency (OCC)
- Federal Reserve Board (FRB)
- Federal Deposit Insurance Corporation (FDIC)
- Consumer Financial Protection Bureau (CFPB)
- Securities and Exchange Commision (SEC)
- NY Department of Financial Services (NY DFS)
- ...

* The FFIEC is a formal US government interagency body that includes five banking regulators – FRB, FDIC, OCC, CFPB and the National Credit Union Administration (NCUA).

Regulatory trends

Focus on third-party risk broadens both inside and outside of financial services to include all firms providing goods and services directly to your organization or to other firms that support your organization.

Advanced Notice of Proposed Rulemaking

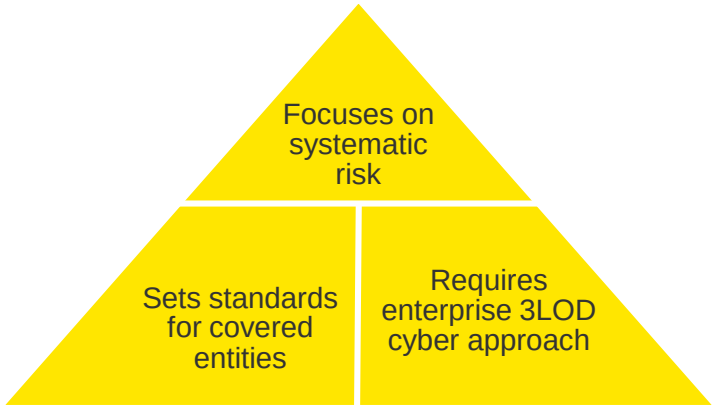
- ANPR's objective is to have effective capabilities in place to identify, manage and reduce cyber risks associated with external dependencies and interconnection risks. Specific to third parties, the proposal includes:
  - Monitor external dependencies and trusted connections based on criticality.
  - Maintain a current database of external dependencies and trusted connections.

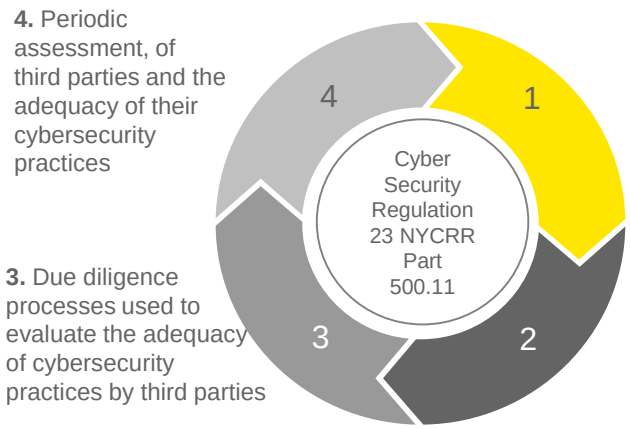
Cybersecurity Regulation 23 NYCRR Part 500.11

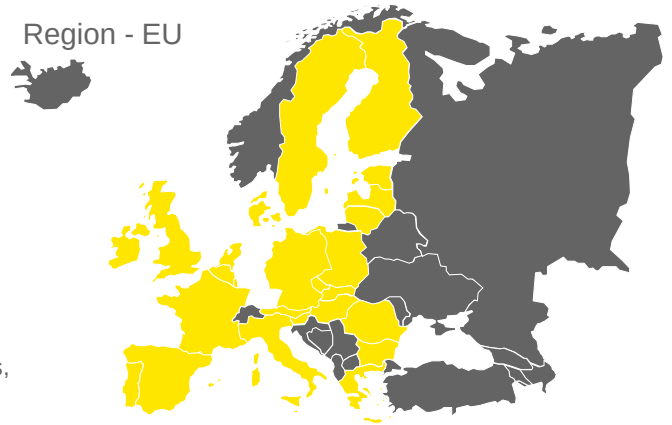
- Each entity shall implement a written policy and procedures designed to provide security of information systems and nonpublic information accessible, or held by, third parties in doing business with the entity.
  - The regulation went into effect March 1, 2017, with section 11 compliance by March 1, 2019
- The policy and procedures should address the following:

General Data Protection Regulation

- GDPR's objective is to heighten the accountability on entities collecting, storing, analyzing and managing personally identifiable information of EU residents.
- GDPR applies to any organization regardless of geographic location that controls or processes the data of an EU resident.







Enhanced cybersecurity and privacy regulation

Industry trends

Industry trends

In the fall of 2017, EY surveyed 54 global institutions with a third-party risk management function in the retail and commercial banking, investment banking, insurance and asset management sectors.

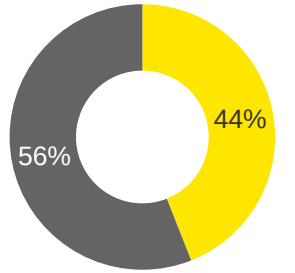
68% of organizations said that **less than 25% of their total third-party population is in scope for their TPRM program.**

96% have not reached **the optimal level** of technology integration.

60% of organizations that identify fouth parties **do not maintain an inventory** for monitoring and governance purposes.

44% of organizations have experienced data breaches that happened at the third party.

Involved in an alliance or consortium to obtain efficiencies in certain areas
Total (54)



Operating Model

57% of organizations reported **having a centralized structure compared to 45% in 2016**.

35% of organizations reported **having a hybrid structure, down from 41% in 2016.**

69% of organizations are **incorporating issues and actions plans, inherent risk assessments, control assessments and related evidence into the scope of their quality assurance function.**

44% of organizations are considering the use of consortiums to drive efficiency in many aspects of TPRM.

6 out of 10 organizations would consider utilizing a common assessment provider.

Third-party population – inventory steadily shrinking

Decreased scope allows sharper focus on higher-risk third parties

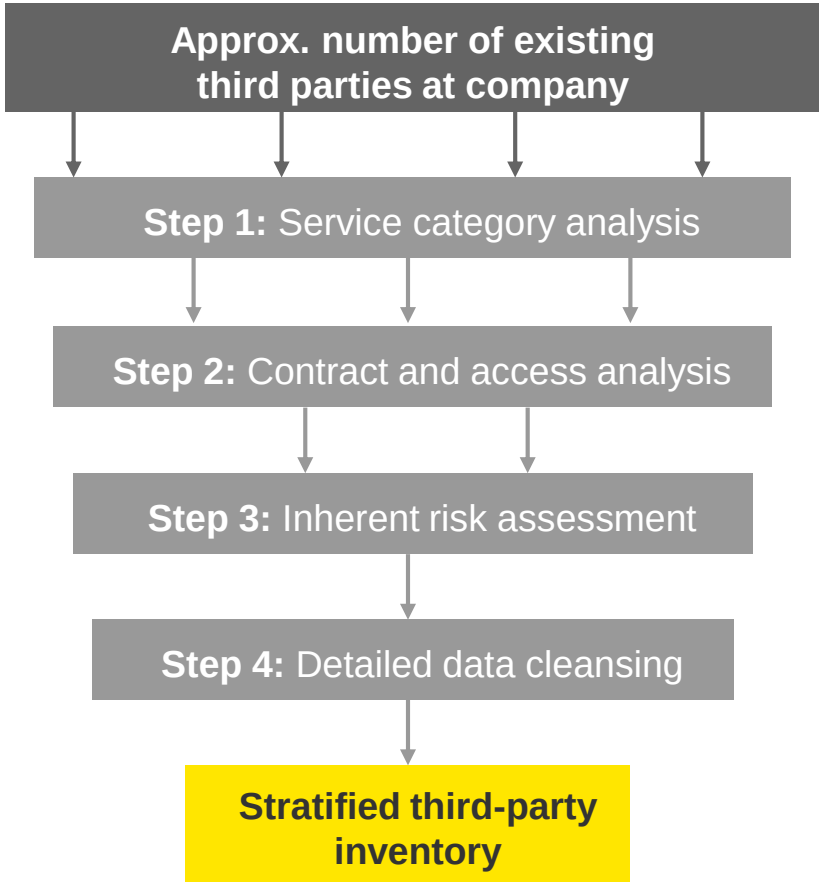
A risk-based approach has translated to fewer third parties in the highest-risk tiers.

At a glance

- The majority (over 68%) of organizations report that only one in four third parties are in scope for their TPRM program, significantly up from the 47% of organizations reported three years ago.
- Only 6% of organizations had all third parties in scope, showing an ease from intense regulatory scrutiny on the concept of "all" third parties being in scope.
- 80% of organizations have less than 10,000 third parties in their inventory, vs. 58% three years ago.

- The majority of organizations have fewer than 10% of third parties in their highest-risk tier.
- 62% of organizations noted fewer than 20% of third parties in their second-highest-risk tier.

Inventory creation strategy



Critical third parties
Defining a critical third party

Defining the appropriate drivers for identifying a critical third party is essential to effectively assess and monitor that third party – the industry has settled on two primary criteria to define critical third parties. This translates to 50% keeping the list to less than 40 third parties, and 75% with less than 80 third parties considered critical.

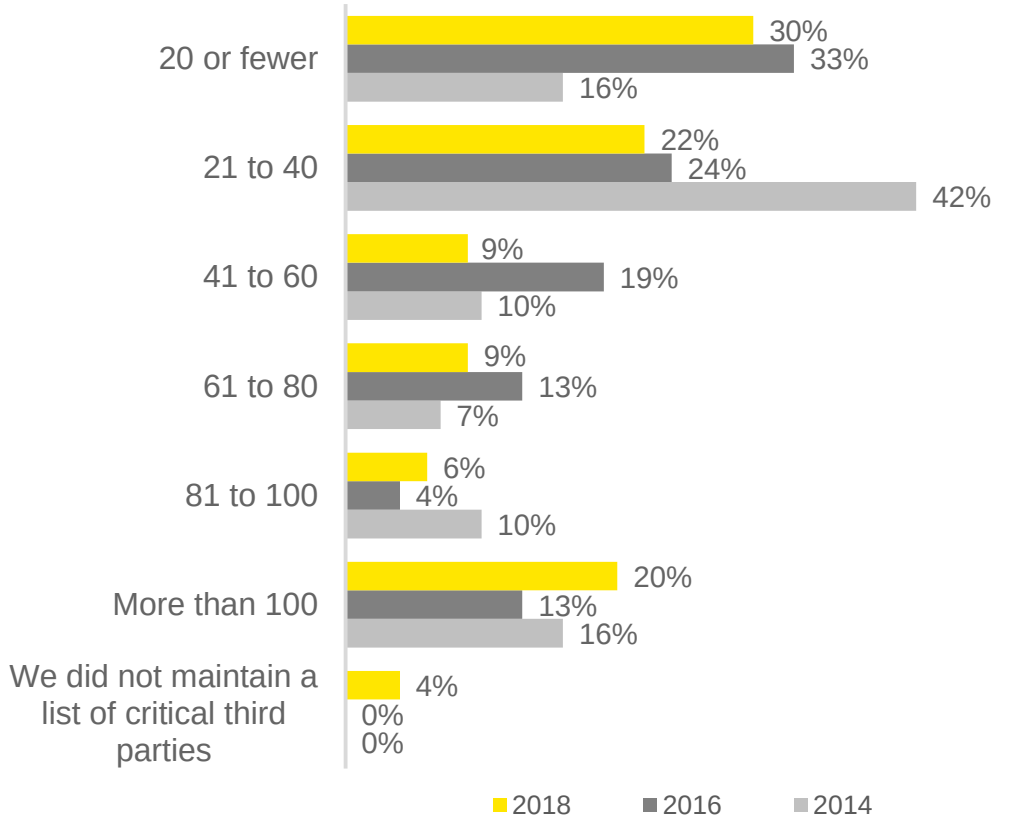
Most important criteria to define critical third party — **2018 | 2016**

1	Potential impact to critical business process	81% | 80%
2	Sensitivity of data involved in providing the service	63% | 74%
3	Inherent risk of the service provided	54% | 63%
4	Strategic importance	28% | 28%
5	Delivery of customer-facing services	26% | 20%

Other important criteria to define critical third party

6 Financial impact (24% | 11%)
7 Operational footprint (9% | 9%)
8 Amount of spend (6% | 7%)
9 Other (4% | 9%)

Number of critical third parties
How many critical third parties are within the organization's third-party inventory?

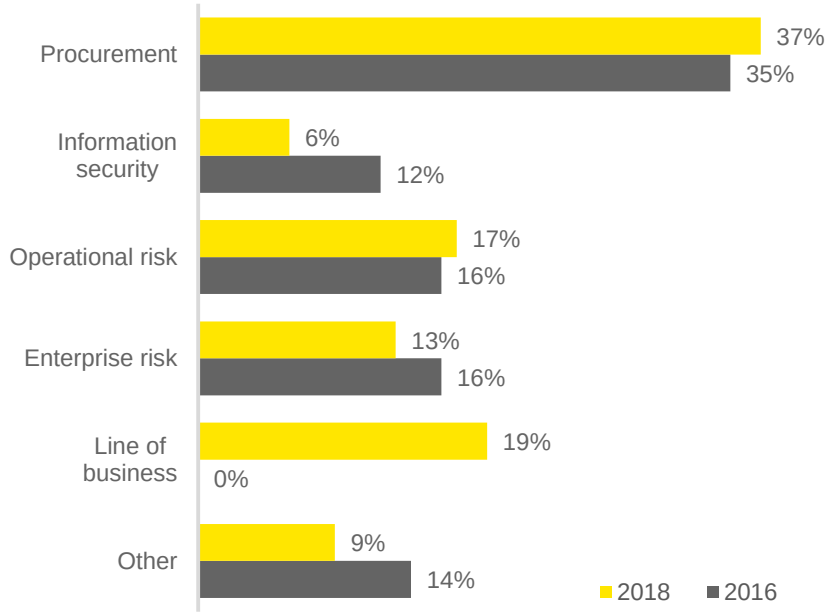


Operating model
Increased centralization of TPRM

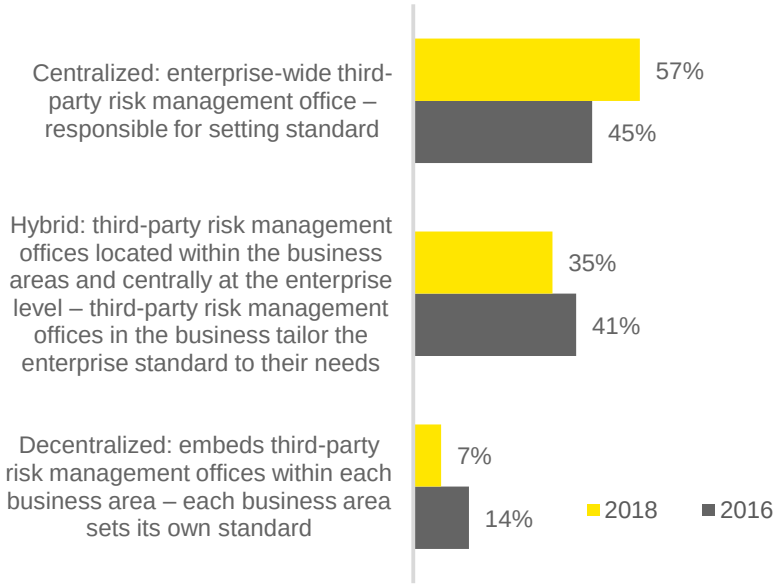
Over a third of organizations said that primary ownership of third-party risk management resides within the procurement function, but there is very little consistency in responsibility and ownership of different functional components of TPRM.

Primary ownership and structure of TPRM function
What area has primary ownership of the third-party risk management function?
How is your third-party risk management program structured

Primary ownership of TPRM program



Structure of TPRM



Centralization of the TPRM function continues to increase, with 57% of organizations having a centralized structure, compared to 45% in 2016. Only 7% of organizations still use a decentralized model, down from 14% in 2016.

Oversight and governance
Reporting and QA

Over the past two years there has been a shift to more mature reporting and quality assurance (QA) functions. On-demand reporting remains difficult for non-critical third parties.

At a glance

- Most organizations (81%) found that reporting on critical third parties was easy and could be done on demand. Reporting on other aspects of the third-party risk management program may take upward of a week or more.
- Less than one-quarter of organizations are reporting third-party breaches or incidents and significant issues to the board, while 60+% report the same to senior management.
- 83% of organizations have a quality assurance function in 2018, up from 72% last year. As programs mature, we noted an increased focus on quality assurance – peaking at mid-maturity – prior to scaling back the focus at more mature TPRM programs.

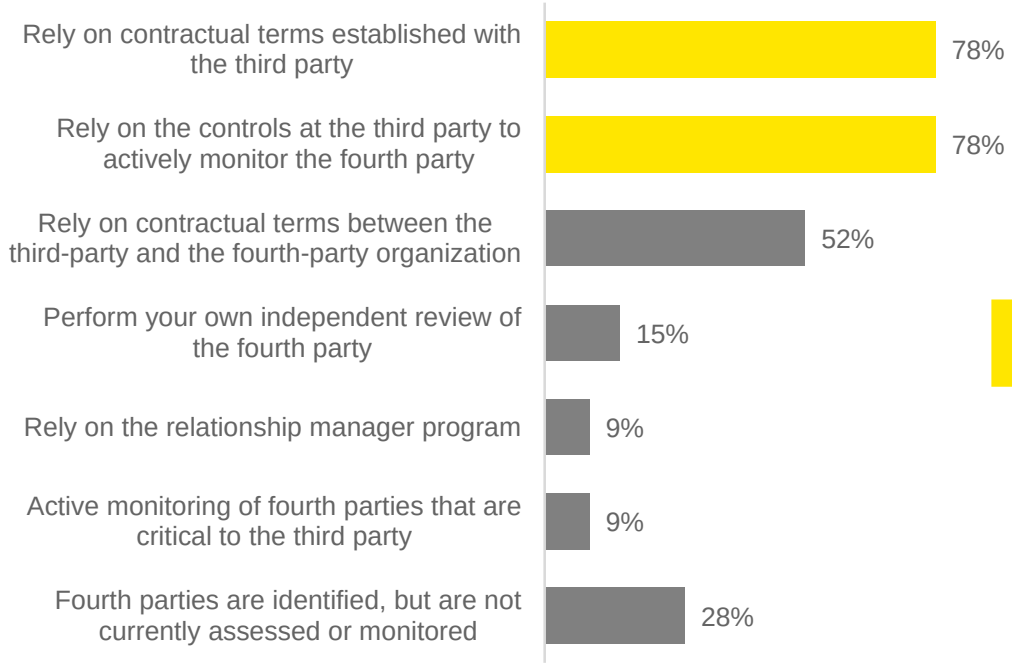
Primary reporting and structure of TPRM function
What activities are performed as part of your organization's oversight and governance program as it related to third-party risk management?

Fourth-party management
A hidden area of risk

Tracking fourth parties remains a major challenge. While 83% of organizations identify fourth parties, 60% of organizations that identify fourth parties do not maintain an inventory for monitoring and governance purposes.

How does your organization assess and/or monitor fourth parties?

Method of assessing/monitoring fourth parties?



Generally, organizations gather information around fourth parties, heavily relying on their third parties during either the precontracting phase or within contracts.

Best-practice approach

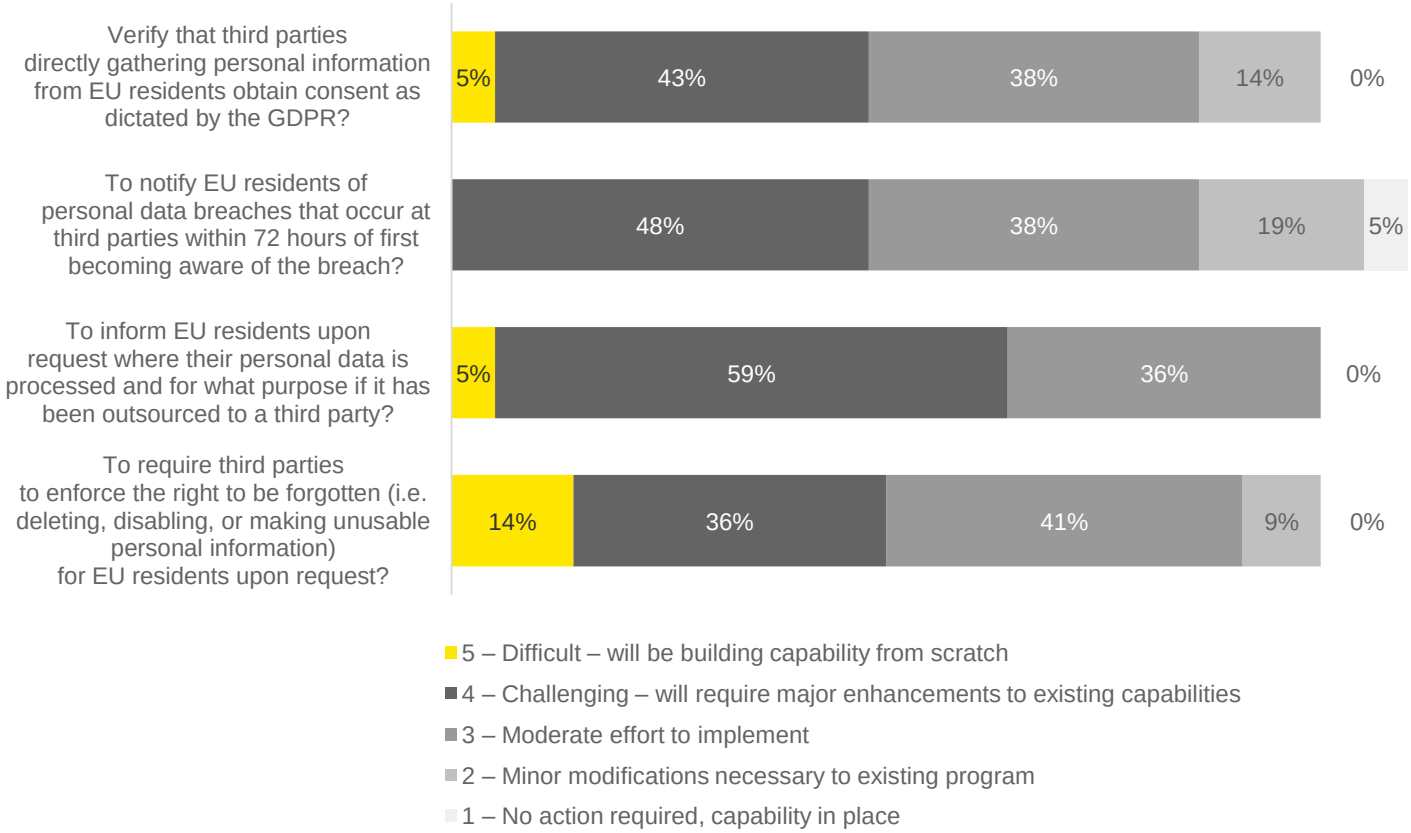
Hone process for risk assessment and oversight focused on direct third-party controls over fourth parties:

- Assess third-party's controls over fourth parties for adequacy and effectiveness as an "add-on" to third-party assessment process
- Focus on riskiest "critical" activities sourced to fourth parties (e.g. collection attorney, subservicer)
- Periodically monitor fourth-party relationships via third party(ies) and perform reassessments as needed
- Enforce contractual terms within third-party contracts to include services provided by subcontractors

Cybersecurity, data breaches and resiliency
Pressure to implement GDPR and ANPR

All organizations responded that it will take at least a moderate effort to implement GDPR requirements for addressing expectations of informing EU residents where their personal data is processed and for what purpose if it was outsourced to a third party.

Difficulty in addressing GDPR guidance



The proposed cyber risk management regulation focused on systemic resiliency, as outlined in the Advance Notice of Proposed Rulemaking issued in 2016 by the OCC, FRB, and FDIC. The ANPR would also be at least moderately difficult for 75% of organizations to implement proper controls.

Major challenges include:

- Monitor external dependencies and trusted connections
- Maintain a current database of external dependencies and trusted connections

Regulatory and internal audit focus

Opportunity to better align internal reviews with regulatory focus

During your organization's most recent regulatory body review, what were the two to three most important areas of focus?

Most important areas of focus		
	Regulatory body	**Internal audit**
Inherent risk assessment	15%	21%
Onboarding activities	8%	13%
Enterprise-critical third parties	29%	15%
Oversight and governance	**42%**	**70%**
Fourth-party oversight	12%	6%
Operating models	8%	15%
Foreign-based third parties	2%	2%
Issue management and/or risk acceptance	10%	9%
Cybersecurity	**42%**	**30%**
Residual risk model	0%	2%
Maintenance of third-party inventory	10%	26%
Consumer protection	8%	2%
Privacy/confidentiality	9%	11%
Nontraditional third parties (e.g., brokers, agents, financial intermediaries)	4%	2%
Our program has not yet been assessed by a regulatory body	**17%**	**4%**

- 42% of regulatory bodies deemed oversight and governance as a top area of focus as compared to 70% of internal audit functions.
- Only 15% of organizations' internal audit reviews viewed enterprise-critical third parties as one of the top areas of focus, compared with 29% of regulatory bodies.

"The regulators really cared about top-down oversight … They really cared about what are your top third parties that had the most impact, and do you have good oversight over them."

– Financial services executive

Industry alliances

Growing trend may disrupt and shift perspectives on TPRM

Of the entities surveyed, 44% have considered using an alliance or consortium to obtain efficiencies in certain areas. Of the 44%:

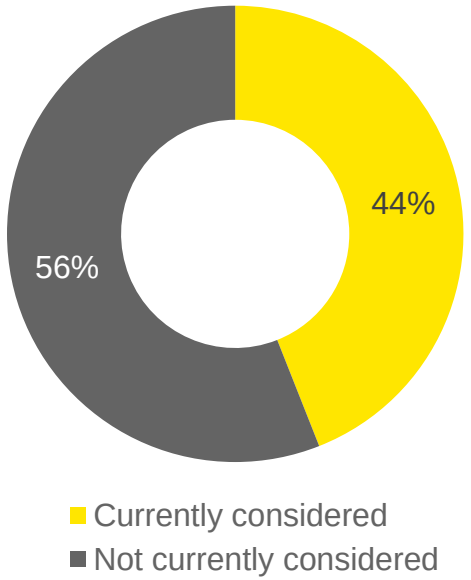
- 75% consider using an alliance for a common assessment framework
- 58% for a common assessment provider
- Half (50%) have considered using common assessment resources

"Firms are eagerly seeking alliances, consortiums and managed services to further improve operational effectiveness and reduce costs. This, along with technology improvement, will be significant efforts in 2018."

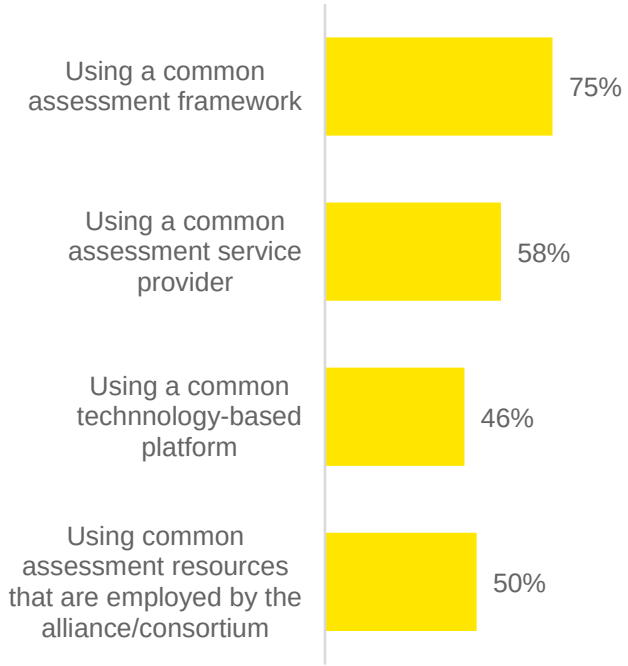
- Chris Ritterbush, Executive Director, Ernst & Young LLP

Is your organization involved in an alliance or consortium seeking to obtain efficiencies in one or more of the following areas?

Involved in an alliance or consortium to obtain efficiencies in certain areas



Areas currently being considered



EY | Assurance | Tax | Transactions | Advisory

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

EY is a leader in serving the global financial services marketplace Nearly 51,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Organization today includes more than 11,000 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America.

EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients.

With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

1805-2679564 BDFSO
ED None

ey.com