


**Can you transform
your third parties'
risk into a
competitive
advantage?**



**The better the question. The better the answer.
The better the world works.**



EY

**Building a better
working world**

Contents

Welcome..... 2

Executive summary..... 4

Six steps to building your TPRM capability..... 10

1. Instill oversight and governance..... 12

2. Get a full view of your third-party inventory..... 14

3. Establish a risk approach and models..... 17

4. Implement policies and standards..... 18

5. Establish and execute TPRM processes..... 20

6. Harness emerging technology to improve risk mitigation outcomes..... 22

Our survey methodology..... 24

Contacts..... 25

Welcome

In today’s connected, digital and highly competitive world, third-party partnerships offer companies the opportunity for greater agility by reducing production or delivery time, while also lowering costs. And companies are seizing that opportunity.

However, while these ecosystems offer incredible opportunities for organizations to provide exceptional customer experiences and drive profitable growth, they also open the door to a host of new risks.

Organizations that will be successful in this new, transformative age are ones that successfully create value from risk across their business and value chain - upside, downside and outside risks. Third-party partnerships are an example of taking an upside risk to deliver strategic value while also being responsible for protecting against downside risks and monitoring outside risks introduced by a related entity.

In the last several years, media headlines have been filled with revelations of cyber attacks and security breaches, regulatory fines, legal actions against top-level executives and reputational damage caused by third-party vulnerabilities. These revelations have shocked senior executives and consumers alike. And they’ve prompted boards and audit committees to pay closer attention. Members of the Audit Committee Leadership Network (ACLN) met in New York to discuss the current state of third-party risk management (TPRM). Their conversation, captured in an ACLN Viewpoints article, underscores the escalating importance of third-party risk and the need to manage it.

Organizations may be able to outsource responsibilities for various functions, but not the accountability. The C-suite is ultimately accountable for the actions of third parties.

Further, the expectation from shareholders and regulators is that boards must know exactly what the company is doing across the globe, which third parties are acting on its behalf and what they are authorized to do. Organizations are increasingly exposed should any inappropriate or criminal behavior take place that jeopardizes the interests of the organization and its stakeholders.

Given its highly regulated environment, the financial services industry has been at the forefront of TPRM. For the last five years, EY has conducted an annual survey of financial services third-party risk professionals to gauge their evolving maturity in managing the increasing third-party risks. This year, EY decided to look beyond financial services and toward other industries that need to introduce or substantively improve their TPRM capabilities. The results of the global organizations we surveyed suggest that many organizations are taking meaningful steps to get ahead of third-party threats. Yet, for the most part, TPRM remains in its infancy for these organizations.

In the pages that follow, we explore how organizations can improve their TPRM posture by taking stock of their current governance structure, identifying and inventorying third-party risk, developing an approach for assessing risk, testing and improving the policies and procedures they have in place, and making certain they have the right capabilities and procedures in place to measure and report their progress.



Vignesh Veerasamy
Global and Americas Advisory TPRM
+1 415 894 8708
vignesh.veerasamy@ey.com



Amy Brachio
Global and Americas Advisory Risk
+1 612 371 8537
amy.brachio@ey.com



Nitin Bhatt
Global Advisory Risk Transformation
+91 806 727 5127
nitin.bhatt@in.ey.com

Questions to consider in addressing third-party risk

1 How does your organization delegate ownership and accountability of third-party risks?

2 Does your organization have a comprehensive catalog of your third parties and third-party risks?

3 Is your organization able to differentiate among third parties based on risk to determine further actions needed to remain protected?

4 Is third-party risk management integrated with your third-party management policies?

5 Does the organization have the appropriate infrastructure and capabilities to effectively manage and mitigate risks?

Executive summary

The escalating need for TPRM

At an annual innovation retreat hosted by EY, panel participants discussed the ingredients necessary for disruptive innovation. Specifically, they argued that the status quo was not only obsolete, it was a recipe for disaster. Organizations have to design ecosystems that bring the outside in while maintaining trust and confidence with key stakeholders. More recently, in EY’s latest semi-annual Capital Confidence Barometer, nearly one in five organizations surveyed indicate that they are looking at joint ventures and alliances to provide both immediate tailwinds and the tools to achieve long-term strategic growth.

These trends suggest that third-party collaboration is not only here to stay, it’s set to accelerate with the

speed of digital evolution. The pace of change in today’s environment will mandate risk communities and ecosystem sharing to stay current and embrace disruption to achieve a competitive advantage in the market. Suppliers, contractors, joint ventures, service providers, brokers, agents and consultants are some of the third parties with whom organizations are forming relationships and building consortiums.

As the need for third-party partnerships grow, so too do the risks. However, the risks lie not only in the relationships themselves, but also in the contracts that bind them together. And organizations are responsible for managing them.



Figure 1: What is TPRM

Third parties pose numerous risks

There are several types of risks that organizations using third parties need to consider, including strategic, operational, financial, geopolitical, regulatory, digital, cyber and privacy, resiliency, and reputational. The level of exposure to these upside, downside and outside risks is based on how organizations are using the third parties.

For example, third parties may have a significant impact to an organization’s operational risks if a third party provides a critical product or service to the organization. What happens if a third party is unable to perform according to their service level agreement due to a disruption in service or a defect in their production line? If a natural disaster occurs, how

does an organization manage business continuity and resiliency risk when third parties are providing the parts and supplies necessary to operate business as usual? What happens if a third party fails to adhere to regulatory and legal requirements and is subject to severe legal penalties and fines?

Risks associated with third parties

Geopolitical risk Risk of doing business in a specific country and includes legal, regulatory, political and social economic considerations	Reputational risk Risk that the organization’s brand and reputation is impacted should an event occur at the third party	Financial risk Risk that the third party cannot continue to operate as a financially viable entity
Regulatory and compliance risk Risk that a third party fails to comply with a required regulation, thus causing the organization to be out of compliance	Digital risk Risk that is associated with the third party’s digital business processes	Cyber and privacy risk Risk that an organization’s data is lost or security is compromised due to deficiencies in the cybersecurity and privacy controls of the third party
Operational risk Risk that a third party fails to meet the organizational needs from a service or product delivery perspective due to deficiencies in the third party’s operations	Strategic risk Risk that the organization’s and third party’s strategic objective are misaligned	Business continuity and resiliency risk Risk of third-party failure on the continuation of business as usual for the organization

Figure 2: Risks associated with third parties

To address the associated risks that third parties pose, organizations need to have a robust TPRM capability in place that is building in trust by design. Figure 3 represents the six foundational components that allow organizations to design and implement an efficient and consistent TPRM capability. Without a consistent and comprehensive TPRM framework, organizations risk reputational damage, incomplete monitoring efforts and increased costs.

The diagram illustrates the components of Third-party risk management. At the top is a large yellow circle labeled "Third-party risk management". Below it, six grey rectangular boxes are arranged horizontally, each connected to the central circle by a line. Each box contains a text label and a yellow icon in a black circle below it. The components are:

- Oversight and governance**: Icon of a building with a dome.
- Third-party inventory**: Icon of a cardboard box with upward arrows.
- Risk approach and models**: Icon of a yellow diamond with an exclamation mark and a flowchart.
- Policies and standards**: Icon of a document with a checklist.
- TPRM processes**: Icon of a hand pointing at a tablet screen.
- Technology, automation and reporting**: Icon of a microchip or circuit board.

A close-up photograph of two chess kings standing on a checkered board. The king on the left is clear glass, and the king on the right is white. Both are highly detailed and reflective. The background is a soft, out-of-focus blue and white.

EY conducted a survey of more than 100 organizations around the globe and across a variety of industries to better understand how organizations manage risk introduced by third parties. The industries include, but are not limited to, consumer products and retail, life sciences, health care, media

Survey topics included program structure, third-party inventory, inherent risk assessments, third-party risk assessments, risk questionnaires, fourth parties, issue management and escalation, reporting and technology, cybersecurity and threat intelligence,

Our findings revealed varying levels of maturity among respondents, depending on their size and how long their TPRM capabilities have been in place. However, overall, most respondents are well behind those with leading-class TPRM capabilities.

TPRM foundational components					
Governance and oversight 	Third-party inventory 	Risk approach and models 	Policies and standards 	TPRM processes 	Technology, automation and reporting
Provides direction for stakeholders in the creation and execution of the program and oversees the function to confirm it is operating as designed	Enables understanding of third-party landscape for automating third-party risk management processes	Establishes that monitoring activities are reflective of the inherent and residual risk assessment associated to third parties and their services and are essential in quantification and illustration of the TPRM program value	Establishes clear roles and responsibilities for all functional owners through the execution of the end-to-end TPRM life cycle; more mature functions embed service and risk management within the overarching third-party management policy and standards for seamless integration	Establishes standard and scalable processes to evaluate and monitor third-party risk levels and control compliance	Increases efficiency, reduces overall cost of the TPRM function and enables continuous monitoring of third-party risks and compliance; additionally, the use of technology increases data integrity and provides seamless and reliable reporting

Key

Level 5: Enhanced
Level 4: Operational
Level 3: Established
Level 2: Planning
Level 1: Initial

Maturity level of leading-class TPRM capabilities
 Maturity level of survey respondents
 Increasing maturity

TPRM foundational components					
Governance and oversight 	Third-party inventory 	Risk approach and models 	Policies and standards 	TPRM processes 	Technology, automation and reporting
Provides direction for stakeholders in the creation and execution of the program and oversees the function to confirm it is operating as designed	Enables understanding of third-party landscape for automating third-party risk management processes	Establishes that monitoring activities are reflective of the inherent and residual risk assessment associated to third parties and their services and are essential in quantification and illustration of the TPRM program value	Establishes clear roles and responsibilities for all functional owners through the execution of the end-to-end TPRM life cycle; more mature functions embed service and risk management within the overarching third-party management policy and standards for seamless integration	Establishes standard and scalable processes to evaluate and monitor third-party risk levels and control compliance	Increases efficiency, reduces overall cost of the TPRM function and enables continuous monitoring of third-party risks and compliance; additionally, the use of technology increases data integrity and provides seamless and reliable reporting

Key

- Level 5: Enhanced
- Level 4: Operational
- Level 3: Established
- Level 2: Planning
- Level 1: Initial

▲ Maturity level of leading-class TPRM capabilities ● Maturity level of survey respondents ↑ Increasing maturity

TPRM survey highlights



42% of respondents manage their TPRM function through a centralized, enterprise-wide TPRM office, with either compliance (22%), information security (21%) or procurement (17%) having primary ownership.



52% say that their TPRM function has been in place for three years or less.



20% of the respondents surveyed have third-party populations of 5,000 or more, with procurement predominantly having primary ownership for these relationships.



30% of organizations experienced a breach caused by a third party within the past two years.

Adoption of technology to support TPRM is still in its infancy; most respondents have not yet adopted third-party provider tools and technology to support TPRM.

Respondents' biggest challenges include a lack of technology, decentralization of responsibilities and budget or funding.



Six steps to building your TPRM capability

To address the associated risks that third parties pose, organizations need to have a robust TPRM capability in place that is building in trust by design – one that identifies third-party relationship owners and guides these owners in how to effectively manage and maintain the risk. Ideally, TPRM activities should be embedded into every phase of the third-party management life cycle. Specifically, organizations will want to consider undertaking the following actions:

1 Instill oversight and governance

Establish a robust governance structure with engagement from the board and C-Suite so that sound risk management practices are embedded into the organization’s culture. Set the tone at the top.

3 Establish a risk approach and models

Adopt risk models according to your organization’s risk appetite and culture. Determine the level of risk your organization is willing to take.

5 Establish and execute TPRM processes

These should be cascaded into each phase of the third-party risk management life cycle.

2 Get a full view of your third-party inventory

Identify, categorize and assess your existing third-party population to effectively manage your third-party inventory.

4 Implement policies and standards

These should outline the purpose and phases of the TPRM framework and define the roles and responsibilities of accountable stakeholders.

6 Harness emerging technology to improve risk mitigation outcomes

Use technology to automate processes, analyze data and report metrics to improve decision-making and understand the operational effectiveness of the TPRM function.



1. Instill oversight and governance

For TPRM to be truly effective, organizations must have the right governance and oversight in place. A governance model helps to improve transparency into and accountability for TPRM and helps make certain that it operates as designed.

TPRM governance defines the vision of the organization's TPRM capability and provides direction for the execution. The operating model for day-to-day functioning should include organizational structure, committees, and roles and responsibilities for managing third parties. In addition, the governance approach should consider how TPRM activities integrate with other risk management functions.

Assign ownership for TPRM

There is no widespread consistency in assigning ownership for third-party risk management responsibilities. According to the results of our survey, primary ownership of the TPRM function typically falls within compliance or information security functions. As TPRM capabilities mature, other functions such as procurement, enterprise risk and legal are integrated.

Organizations can use a centralized, decentralized or hybrid structure to manage their TPRM capabilities. The structure tends to vary depending on the organization culture, operating model and maturity of the function.

For more than half of respondents, the TPRM function has been in place

for three years or less. Most of these organizations have opted to establish their TPRM capability with a centralized structure. Approximately 45% of respondents whose function is three years or older use a hybrid approach, with the business area becoming increasingly involved in supporting more centralized TPRM activities. A centralized structure decreases redundancies and can be managed holistically. In a decentralized structure, the onus is on the individual business units for managing the risk. This can lead to an inconsistent use of standards and duplication of resources and work.

The number of full-time resources dedicated to TPRM capabilities can vary based on the size of the organization. For example, 40% of respondents with fewer than 100,000 employees have between 1 and 5 full-time resources in their TPRM function. However, the number of dedicated TPRM resources climbs dramatically for respondents with more than 100,000 employees, with 56% reporting that they have more than 25 people supporting the function.

Establish a governance structure

To establish an effective oversight and governance structure, organizations should look at their TPRM framework in the context of the three lines of defense. A clearly defined three-lines-of-defense model helps the TPRM capability to operate effectively in monitoring and reducing risk.

Employees responsible for the first line of defense own the third-party business relationship and day-to-day oversight. They are relied upon to identify, measure, monitor and report risks generated by business third-party relationships.

The second line of defense team designs and owns the third-party risk management framework. They provide an independent, risk-based viewpoint and guide the first line of defense in risk responsibilities.

Those responsible for the third line of defense independently assess adherence to the TPRM framework and provide assurance that the third-party risk management process is functioning as designed.

The board is ultimately accountable for third parties and their issues and risk. Organizations with leading-class TPRM capabilities also set up a TPRM oversight committee that reports up to the board.

Involve key stakeholders to improve success

Organizations should identify critical stakeholders and appropriately engage with them to enhance ongoing TPRM success. Organizations will also want to seek support from business unit leaders as champions to drive adoption. TPRM activities need to build relationships, increase awareness and integrate third-party risk management practices into day-to-day business processes.

Board-level involvement is critical for stakeholder buy-in. Unfortunately, third-party risk is not yet on the board's agenda within most organizations. Only 22% of survey respondents report breaches to their board while 55% report breaches to senior management.

“We have full support from the board and senior management. We have a dedicated meeting with the senior management team every month to review all third-party risks and how they are being dealt with or mitigated. We have also tried to educate at least the audit committee. And as we've educated them, they've been fully supportive.”

– EMEIA, Power and Utilities respondent



42% of respondents operate under a centralized TPRM structure or from an enterprise-wide TPRM office.



52% of respondents say that their TPRM function has been operational for three years or less.



22% of respondents report breaches to their board.

Future trends:

- 1. Third-party risks will get more board-level attention.** Organizations typically provide third-party risk reports to senior management. However, relatively few escalate issues to the board level. As more organizations realize that board-level involvement is an important factor in the success of TPRM, they will feature it on the board agenda.
- 2. Sector-based alliances and consortiums will continue to transform the TPRM function.** Sector-based consortiums and alliances provide repeatable third-party risk management capabilities that multiple participating organizations within a sector can use. Consortiums seek to more effectively mitigate third-party risk, while reducing the overall cost and burden on the industry and on third parties. Sector-based consortiums are currently, and will continue, transforming the TPRM function. Nearly half of the respondents we surveyed indicate they are looking to gain efficiencies by joining an industry alliance or consortium.

2. Get a full view of your third-party inventory

A surprising number of organizations do not have a full view of their third-party inventory. Organizations have inventories that are incomplete, spread across multiple systems and departments, and lack a single source of truth. However, before organizations can look to effectively manage their third-party risks, they first need to identify their third parties and the respective third-party owners, as well as categorize their vendor inventory.

Identify third parties and their relationship owners

For organizations that do not have an inventory and are trying to build one reactively, they can leverage existing third-party data that groups such as procurement, compliance, legal or existing business units maintain. Using invoice or payment data, contract management databases or enterprise resource planning (ERP) systems can provide the foundation for this inventory. Although many organizations do not have one system that contains this data, they can still build connections and relationships among the different systems to feed into a single inventory management system.

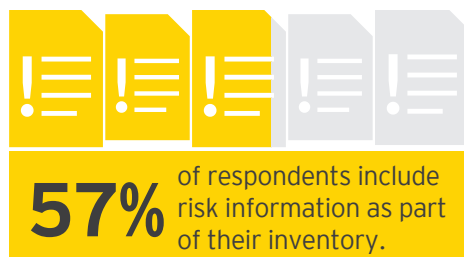
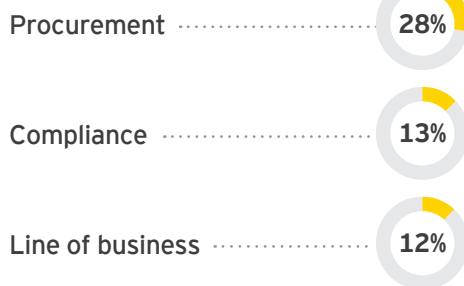
Categorize vendors

Not all third parties are the same; segmentation allows organizations to prioritize their efforts and ultimately how vendors should be managed from a risk perspective. This is especially true when the number of third parties

is large and growing. One in five of survey respondents have third-party populations of 5,000 or more.

At the most basic level, organizations initially segment their inventory by new and existing third parties. These two groups should be managed and assessed differently. After this initial segmentation, organizations should take a more detailed look into their populations by grouping vendors by other, more specific criteria, such as criticality, service type and cost, and business units that receive the third-party services. Once they've collected the risk information, organizations should categorize third parties based on level of risk. This will drive downstream risk management activities.

Who owns the third-party inventory?



Collect relevant risk information

In a mature organization, a third-party inventory goes beyond a master list of vendors containing basic purchase-to-pay data. A mature inventory offers a view of the risks each vendor brings to the organization. This type of inventory includes dynamic information, such as service description details, date service started, spend information, third-party contract or agreement, accountable relationship owners and executives from the contracting organization, a list of vendor representatives, sub-vendors (or fourth parties), and a summary of key risks associated with each third party.

Maintain a real-time third-party inventory

The third-party inventory needs to be maintained as it is constantly changing, with third parties being added and removed or services expanding and reducing. Maintaining an accurate and complete third-party inventory can serve as the foundation for automating third-party risk management processes. Organizations will want to review the inventory on an ongoing basis for new, terminated, inactive and rogue vendors ("rogue" meaning where businesses engage the vendor outside of the contracting protocol) and compare this to the third-party invoice data.

The most effective TPRM approach will have direct inputs from risk management, compliance and business units to maintain a real-time and robust third-party inventory.

"Understanding what risks your third parties pose to your organization is half the battle, but first you must ensure your inventory is accurate."

– North America, Health Care respondent

Future trend:

Business intelligence will drive operational change and improve decision-making. Organizations are increasingly using third-party risk data, predictive modeling, statistics and visualization to generate insights that help procurement and supply chain to make better decisions. Data gathered from TPRM activities can also be used to provide third-party risk intelligence that drives operational change and reduce risks throughout the vendor life cycle.



3. Establish a risk approach and models

Based on the organization's risk appetite, organizations should determine the risks that are relevant and the models to use. These risks should align with the organization's risk identification strategies and enterprise risk management program.

As organizations develop a clear view of their third-party landscape through a robust inventory, it is important to differentiate among third parties based on risk and understand what further actions organizations may need to be taken to remain protected. Mature organizations have an established risk universe (geopolitical, reputational, financial, regulatory and compliance, cyber and privacy, operational, strategic, digital, business continuity and resiliency) that helps to identify which risks should be used to evaluate third-party relationships and the level of risk that the organization is willing to take. These organizations feed risk information collected about third parties into risk models that allow them to qualitatively and quantitatively assess the risks and focus their efforts on monitoring and managing higher levels of third-party risk. The risk models also help to classify third parties based on defined levels of risk (e.g., low, medium, high, critical).

Organizations should categorize third parties based on the level of risk in their third-party inventory. A third party's ranking within an organization's risk model drives the monitoring activities that organizations perform.



59%

of respondents have three or fewer risk tiers. Among respondents that have had a TPRM function in place for more than five years, 87% use three or more risk tiers.



24%

of third-party risks are classified as critical or highest risk.

“Organizations that methodically identify, assess and respond to external risks that have the potential to impact their business strategy are better equipped to define risk responses that reduce the negative impact of the risk while helping maximize the organization's potential.”

– EY, *Insights on governance, risk and compliance: external risks, 2017*

Future trend:

Organizations will need to consider a broader range of upside, downside and outside risks and break down the organizational silos. In an increasingly digital and technology-driven world, it is vital for organizations to understand and react to information security and privacy risks. Survey results indicate that 68% of respondents are already collecting information on the data and systems access held by their third parties. Further, 52% of respondents say that their information security function is involved in the design or maintenance of the inherent risk assessment process. However, as third-party risk management continues to evolve, the most mature and risk-savvy organizations will expand their focus beyond information security and regulatory compliance and aim to cover a broader, more inclusive set of risk factors. Most importantly, the interconnected nature of risk across the enterprise means that TPRM cannot function in a silo. Organizations will be better served aligning their enterprise risk management, TPRM, cybersecurity and other risk-related functions and capabilities to provide a holistic view on risk.

4. Implement policies and standards

Policies and standards establish clear roles, responsibilities and expectations for all stakeholders involved in an organization's TPRM initiatives, internally and externally. And yet, according to our survey, 70% of respondents cite some level of difficulty in formally establishing policies, procedures and guidelines, as well as maintaining consistent compliance with the policies that are in place.

Policies and standards are not sufficient without the support of executive management. The executive management team should

be responsible for enforcing the requirements stated in the policies and standards and driving accountability for key stakeholders.

It is critical for all internal stakeholders to understand their responsibilities when engaging a third party, the risks associated with doing business with an external party and the consequences of not complying with the organization's policies and standards to achieve effective TPRM execution.

TPRM policies and standards must clearly state the TPRM purpose and

approach, provide definitions of third parties and related key terms, define key roles and responsibilities, outline the TPRM framework, describe all phases of the TPRM life cycle, document the system(s) of record used to manage the third party and explain the escalation protocols for non-compliant stakeholders or third-party issues. Policies and standards should be reviewed and approved by the executive management team on an annual basis at minimum.



70% of respondents cite some level of difficulty in formally establishing policies, procedures and guidelines, as well as maintaining consistent compliance with the policies that are in place.

“Organizations need policies and procedures to set the standards and guidelines for managing third-party risks across the enterprise. Without it, you cannot expect resources to understand their roles and responsibilities when it comes to managing third parties.”

– North America, Health Care respondent



5. Establish and execute TPRM processes

For policies to have their biggest impact, organizations should have in place a risk management framework that guides third-party relationship owners to more effectively manage the relationships and their underlying risks.

As shown in the graphic below, an effective third-party risk management process follows a continuous life cycle for all relationships and incorporates the following phases. The following framework aligns foundational risk elements throughout the third-party risk management life cycle. Industry standard frameworks such as those published by the International Standards Organization (ISO) and National Institute of Standards and Technology (NIST) can help organizations build their initial framework by adopting a globally accepted risk management structure and methodology.

Implementing an industry standard framework is a good start, but it’s not enough to build a comprehensive TPRM capability. The chosen framework needs to be adjusted and enhanced based on the organization’s industry, competencies, mission and TPRM vision.

Most organizations focus on risk management activities during the due diligence and monitoring phases. However, organizations need to embed TPRM activities across the third-party risk management life cycle. More mature functions embed service and risk management within the overarching vendor management policy and procedures for seamless integration and streamlined execution.

Sourcing begins the third-party risk management process by working with stakeholders to define business requirements and kick off the bidding process for third parties. During this

process, sourcing performs an inherent risk assessment to understand the risks associated with the third parties.

TPRM activities primarily occur during the due diligence, onboarding and monitoring phases, where the organization selects and onboards the third party after understanding the risks of managing the vendor. Key activities in these phases include an inherent risk assessment, residual risk assessment and risk response management.

This process is not only for new third parties, as existing vendors must also undergo risk assessments to identify their risk rating and be included in the monitoring phase according to the level of risk. Organizations should apply a consistent approach to monitor vendors and escalate issues and risks to the appropriate oversight and governance groups. If an organization needs to terminate a third party, it

should perform a close-out assessment to understand the level of risk exposure that the third party’s termination poses to the organization. Policies, procedures and standards should outline the key TPRM activities so that the process is communicated and implemented across the organization.

Examine inherent third-party risk
Inherent risks are the risks associated with providing a product or service regardless of the controls and mitigating factors that a third-party may have in place.

Organizations typically evaluate inherent risks using risk assessments to determine where each service falls on the organization’s third-party risk spectrum. Inherent risk data often includes a view of critical risk factors such as product and service location, relevant regulations, financial, operational and reputational impact (e.g., HIPAA, PCI DSS, GDPR, UK’s Cyber Essentials), sub-vendor (fourth party) involvement, business continuity, data and systems access, and access methods. Using this information, a risk model can determine the third party’s overall inherent risk standing. To calculate this inherent risk rating, organizations develop questionnaires to assess the risk that the third party would pose to the organization.

Look for residual risk
Based on the inherent risk rating, organizations can then conduct varying levels of residual risk

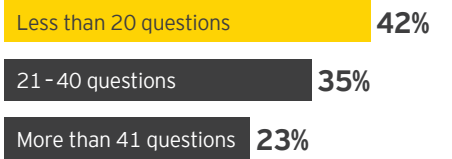
assessments. Residual risk assesses a third party’s controls and mitigating factors. When effective, controls typically reduce the overall level of inherent risk associated with a third party’s products and services. A lower residual risk may decrease the level of monitoring activities required, even when the product or service risk is inherently high.

Organizations can perform residual risk assessments using an in-depth questionnaire, on-site visits or phone meetings. For the most critically rated third parties, 37% of respondents say their organization elects to perform their third-party risk assessments on-site. Only 22% conduct on-site assessments for third parties that are rated lower than critical. For risks that are high but not critical, 60% of respondents say their organization conducts a full-scope remote assessment, an increasing trend that uses fewer resources and results in a similar level of assessment quality.

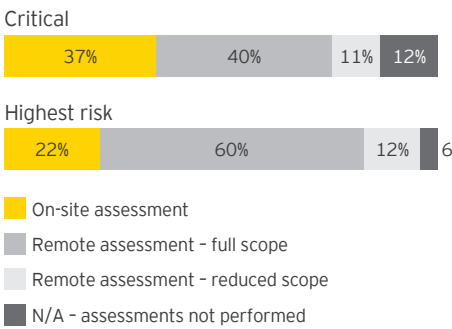
More than **40%** of respondents surveyed use ISO or NIST as a baseline, and **21%** use a proprietary framework to develop their questionnaires.

Once organizations have identified and assessed the risks, they need to put the building blocks in place to manage them. Organizations can work with the third parties to accept, remediate or mitigate these risks.

Number of questions included in the inherent risk assessment questionnaire



Method typically used to conduct a third-party risk assessment for critical and highest risk third parties



“Siloed” approaches to third-party risk management usually lead to contract governance gaps, overlapping monitoring programs and increased execution costs.

– EY, *Third-party risk management: moving from a compliance obligation to a source of competitive advantage, 2018*



Note: Third-Party Risk Management aspects displayed in bold.

Figure 5: TPRM key activities

6. Harness emerging technology to improve risk mitigation outcomes

In today’s technology-driven world, TPRM capabilities need to include technology tools that can automate processes and analyze the data that TPRM activities generate. Many companies still use Excel spreadsheets and manual processes to maintain and report their third-party inventory and TPRM process. Organizations are using on-premises and Software as a Service (SaaS) solutions, although more organizations are leaning toward the latter. SaaS solutions are more efficient and cost-effective.

Choose the right third-party technology
Overall, organizations are looking for TPRM technology that offers improved cost efficiencies and scalability to meet a growing third-party population. The technology also needs to integrate seamlessly with other organizational systems and have an intuitive and user-friendly design and interface. Although there is no overriding favorite system when it comes to technology tools, 12% report using SAP and 13% elect to go with their own proprietary tool.

Increase efficiency
Robotic process automation (RPA) is introducing high-impact innovations into the TPRM industry that allow organizations to significantly decrease process time while increasing the volume of assessments. RPA can then further help streamline operations by eliminating manual tasks, repetitive activities and process bottlenecks. Organizations can then focus their time building their third-party risk inventory to include all types of risks, such as information security, geopolitical, financial, regulatory and reputation.

Functions	Archer on-premises	Archer VRM cloud	SAP/Ariba	Oracle	BWise	Hiperos	ProcessUnity	Prevalent	Proprietary	None
Sourcing activity	4%	0%	24%	11%	0%	1%	0%	0%	12%	48%
Inherent risk assessment	1%	1%	4%	1%	2%	5%	4%	1%	13%	68%
Contract repository	0%	0%	18%	6%	0%	0%	0%	0%	16%	60%
Primary third-party inventory	5%	0%	12%	7%	0%	1%	1%	0%	13%	61%
Third-party risk assessment facilitation tool	6%	1%	2%	0%	0%	2%	4%	0%	13%	72%
Issue or risk response management tool	7%	2%	4%	0%	1%	1%	4%	0%	13%	68%

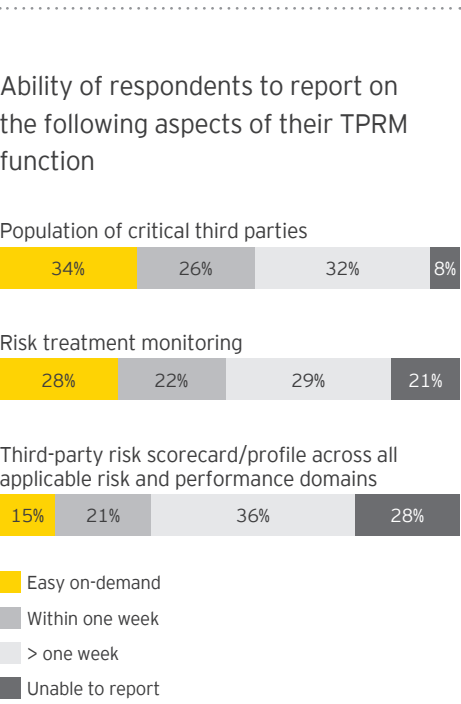
Report results
Organizations can use real-time reporting to provide timely updates to the business, senior management and the board. Some of the more mature organizations are able to break down their third-party inventory by reporting common risk themes within the third-party community and service type. This information allows mature organizations to provide details to procurement and contracting so that they can identify these risks at contract initiation.

Currently, only 34% of respondents say they have on-demand reporting for critical third parties; only 28% can report on their risk treatment distribution in the same way.

The next step for organizations will be to leverage technology for predictive modeling (i.e., indicating areas of emerging risk), real-time statistics that will allow management to focus budgets in the right areas, and visualization to provide leadership with simple intuitive graphics for insightful and effective decision-making. Organizations that invest in technology for real-time reporting and automation will be one step ahead of organizations that continue to rely on manual activities. The following figure displays what capabilities organizations have today for reporting third-party risks.

“Technology has allowed us to streamline the process, digitize information to help organizations make informed business decisions and more efficiently link to external data sources and providers.”

– EMEIA, Health Care respondent



Future trend:

A tectonic technology shift will move TPRM from manual to automatic.

As the TPRM industry follows the accelerating digital wave from on-premises technologies to cloud-based and SaaS platforms, manual processes and spreadsheets will give way to automation and analytics. The benefits of automation and real-time analytics include cost reduction, increase in productivity, high availability and reliability, and performance growth. These benefits far outweigh the cost of acquiring these technologies – an opportunity that organizations are seeing and seizing.

Our survey methodology

EY conducted a survey of 101 organizations around the globe and across a variety of industries, each with a function to manage third-party risk. The industries include, but are not limited to, consumer products and retail, life sciences, health care, media and entertainment, technology, power and utilities, diversified industrial products, and government and public sector.

In this survey, we asked participants to respond to questions within several key areas of their respective TPRM programs. Topics included program structure, third-party inventory, inherent risk assessments, third-party risk assessments, risk questionnaires, fourth parties, issue management and escalation, reporting and technology, cybersecurity and threat intelligence, and future challenges.

To gather more in-depth insights and examples, we conducted follow-up interviews with select participants covering topics such as drivers for success, operating models, board involvement, use of technology and planned investments in their TPRM programs and functions.

We extend a personal note of thanks to our survey participants for taking the time to share their experiences.

Respondent profile		
Total	101	
By industry	Number of respondents	%
Consumer products and retail	19	19%
Technology	17	17%
Life sciences	11	11%
Health care	9	9%
Media and entertainment	9	9%
Telecommunications	6	6%
Power and utilities	5	5%
Diversified industrial products	5	5%
Government and public sector	3	3%
Other*	17	17%
By region		
North America	72	72%
Europe, Middle East, India and Africa (EMEIA)	23	23%
South America	4	4%
Asia Pacific (APAC)	2	2%
By organization size		
Fewer than 24,999	63	62%
25,000 to 50,000	16	16%
50,001 to 100,000	13	13%
More than 100,000	9	9%

* Industries such as oil and gas, HR services, mining and metals, automotive, logistics, chemical, real estate, hospitality and construction were grouped as "Other" due to insufficient sample size. Numbers may not add to 100% due to rounding.

Contacts



Vignesh Veerasamy
Global and Americas Advisory TPRM
+1 415 894 8708
vignesh.veerasamy@ey.com



Netta Nyholm
EMEIA Advisory TPRM
+49 221 2779 16427
netta.nyholm@de.ey.com



Glen Gooding
Asia-Pacific Advisory TPRM
+61 2 9248 5789
glen.gooding@au.ey.com



Harald deRopp
Japan Advisory TPRM
+81 3 3503 1110
harald.deropp@jp.ey.com



Matthew Moog
Global and Americas Financial Services TPRM
+1 201 551 5030
matthew.moog@ey.com



Amy Brachio
Global and Americas Advisory Risk
+1 612 371 8537
amy.brachio@ey.com



Nitin Bhatt
Global Advisory Risk Transformation
+91 806 727 5127
nitin.bhatt@in.ey.com

Notes

This image shows a blank sheet of white paper with horizontal ruling lines. The lines are evenly spaced and extend across the width of the page. There are no margins, text, or other markings on the paper.[illegible]

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.

© 2018 EYGM Limited.
All Rights Reserved.

EYG no. 03111-181Gbl

1805-2676748

ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax or other professional advice. Please refer to your advisors for specific advice.

ey.com

