ERM and Third-Party Risk

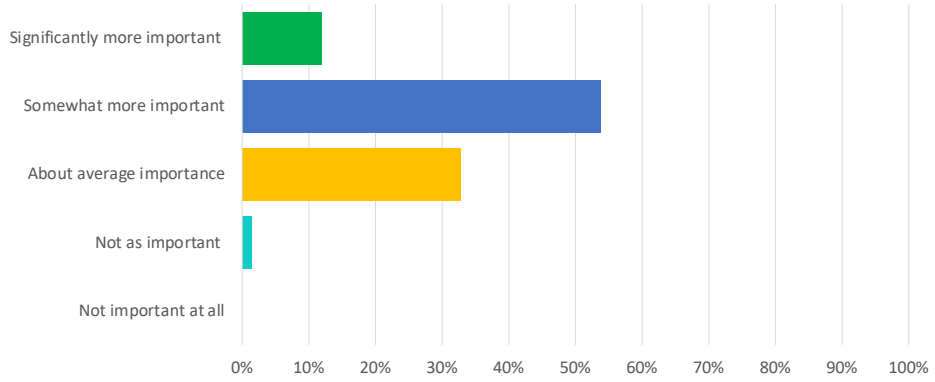
White Paper Series
St. John's University, Tobin College of Business
Center for Excellence in ERM
Dr. Paul L. Walker

Third Party Risk: A Growing Risk that Organizations are Rethinking

In May 2022, more than 100 risk leaders gathered virtually to discuss supply chain and third-party risk management (hereafter, TPRM) at the 11th ERM Summit hosted by the Center for Excellence in ERM at St. John's University. Supply chains have been hit hard by energy changes, global conflicts, and inflation and some supply chains that seemed efficient and stable for years ended up in big trouble due to these global disruptions. Because of this it's not much of a surprise that companies are rethinking supply chains, their business approaches, and all third-party risks.

Third party risks can be quite large. Risk leaders attending the Summit revealed that while some only listed that they had a few hundred third parties, others listed thousands, or tens of thousands, and one even stated, "countless." Furthermore, many also noted that a significant percentage of those third parties are considered critical, with a few organizations noting that up to 50% of their third parties are considered critical. One risk leader noted that third-party risk is a top three board risk issue and suggested that many organizations do not know their exposure. A survey of the Summit attendees found that **over 90% agreed that third-party risks have increased and over 60% believed that third-party risks are more important than other risks, in essence, making this a top risk and a likely subject of discussion for boards at many organizations.**

How important is third-party risk management (TPRM) to your organization relative to other key risks you are tracking?



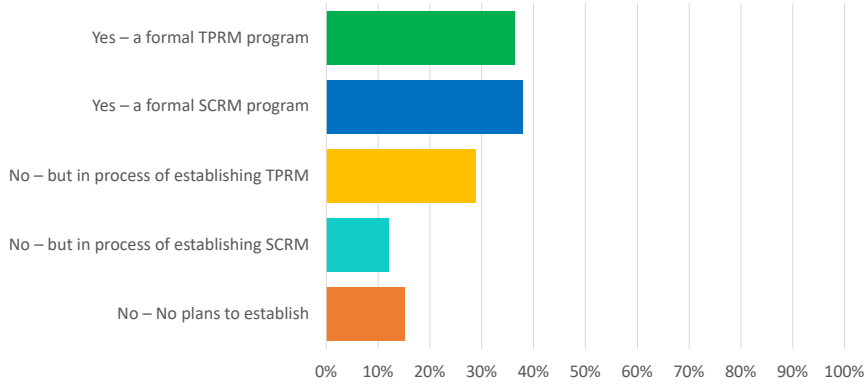
When asked *which* third-party risks were significant to their organizations, the risk leaders ranked cyber security as the most important. Other risks were ranked as follows (in descending order):

- Cyber security
- Data privacy
- Business continuity
- Business disruption
- Supply chain
- Compliance with laws and regulations
- Reputation
- Concentration risk (e.g., third-party dependency)
- Contract
- Legal, and
- Solvency.

Building and Enhancing TPRM

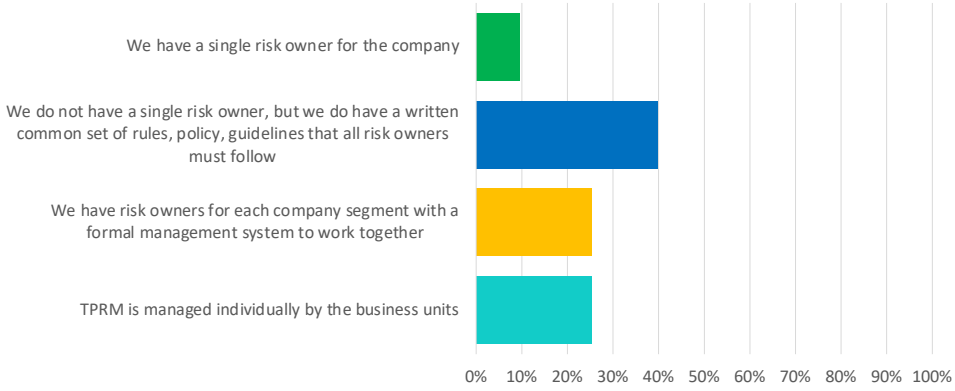
Companies are working to improve TPRM. In fact, **80% stated they are planning on building or enhancing their third-party risk programs** within the next year. These numbers are interesting because many already had a formal supply chain or third-party program so the message seems to be if you do not have a program, then build one; if you do have one, then improve it.

Does your organization have a formal third-party (TPRM) or supply chain risk management (SCRM) program? (Check all that apply.)



Building and improving TPRM requires addressing some big issues. One issue is determining the owner of the risk. This is not an easy question and the answer likely varies by company size, industry, and complexity and nature of the risk. As seen below, around 10% have a single risk owner, around 25% have a risk owner for each company segment, and another 25% have the business unit responsible for the risk. No matter who owns it, one recommended approach is to have a common set of rules, policies, and guidelines that any risk owner can follow. An effective ERM leader seems important in this area especially if a common approach across the enterprise is needed.

Is the TPRM approach to have a single risk owner for the enterprise or to have ownership embedded in the business area?



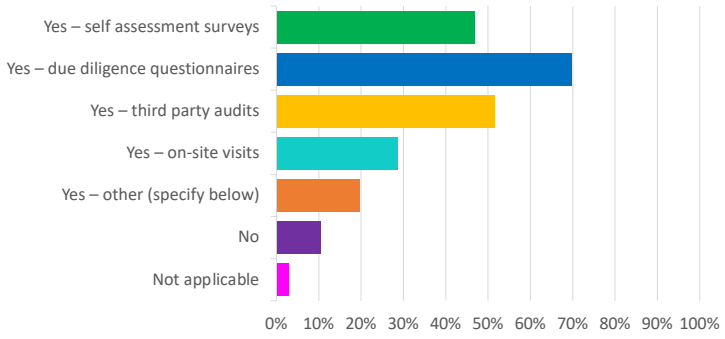
ERM Involvement with TPRM

ERM leaders can play a critical role in helping business units or other owners see and learn how TPRM is connected to other enterprise risks that face the organization. What is important for some is that the ERM leader become involved with TPRM in one way or another; it cannot be a siloed risk. Appendix 1 shows the raw responses when risk leaders were asked how to engage with TPRM and several themes emerge from the answers. **The first theme was to have a conversation about the risks.** Examples of those conversations included risk leaders collaborating with TPRM, TPRM consulting with ERM, having consistent interaction, sharing input, meeting regularly, and developing a partnership.

Another theme that emerged was to take action. One action that was mentioned was including TPRM as part of the annual risk assessment and mapping exercise. Others suggested conducting third-party risk assessments or doing specific projects or initiatives on third party or related emerging risks. More suggested actions included reviewing new business or vendor changes and participating in the development of a third party or supply chain risk program. When asked about how they assess third parties, over 40% used surveys, almost 70% used questionnaires, and about 50% used third party audits. Additionally, 45% noted that they

differentiate between essential and non-essential third parties and 23% noted that they have separate risk appetite statements for third party risks.

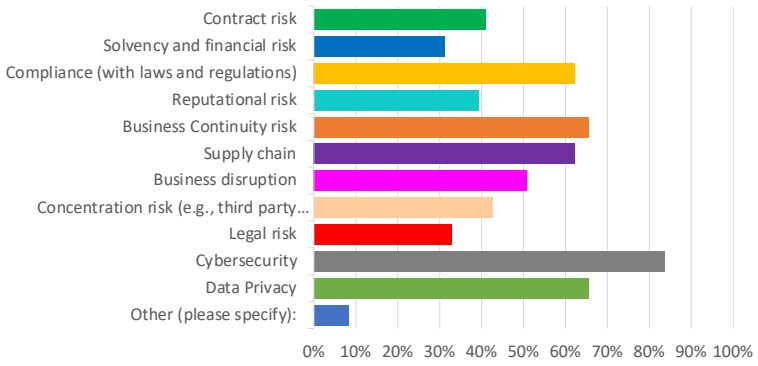
Do you have a formal process for assessing third parties as High Risk? (Check all that apply.)



One theme seemed to focus on applying an ERM framework. Several risk leaders mentioned the importance of applying such a framework to ensure consistent approaches in managing the organization's risks. Similar comments addressed sharing risk protocols, leveraging the ERM framework, integrating third party risks into the ERM process, determining which third party risks are enterprise level risks, providing consistent oversight of third party and other risks, and aligning on taxonomy or escalation.

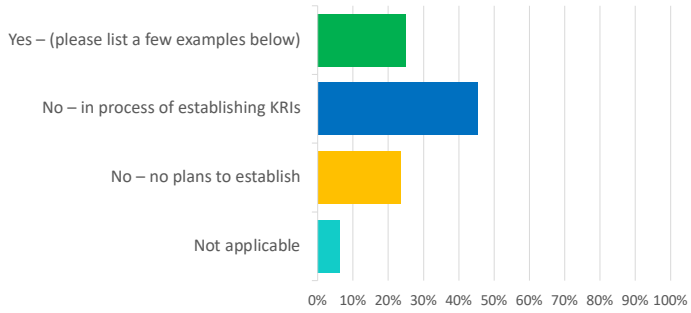
All this involvement and assessment naturally led to determination of third-party risk categories, reporting, and key risk indicators. Popular risk categories that risk leaders are tracking include cybersecurity (83%), business continuity (67%), data privacy (64%), compliance (62%), supply chain (61%), and business disruption (50%).

What are the main third-party risk categories that ERM is tracking? (Check all that apply.)



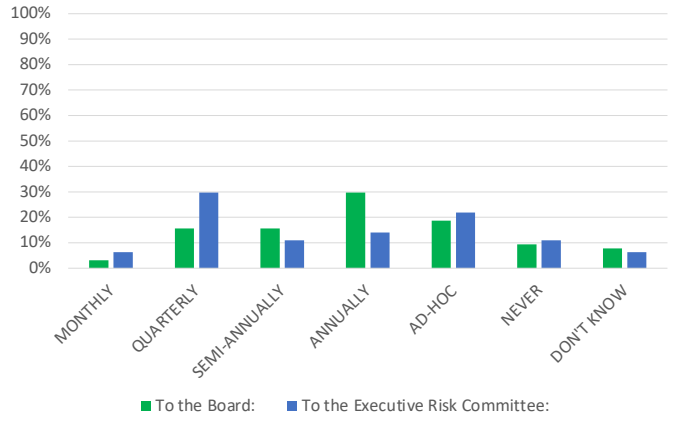
Key risk indicators are important too. In addition to tracking the risks, 25% were using key risk indicators and another 46% were in the process of establishing key risk indicators. Some metrics mentioned for the key risk indicators included supply buffers, supplier stability rating, missed shipments, geographic concerns, financial health, supply chain continuity, contractor safety, contractor compliance, impact of remote work, location, single/sole sources, overall risk ranking (based on more detailed scoring), risk and impact matrices, quality, performance, and cybersecurity events impacting the supplier's customers.

Does your organization use Key Risk Indicators to monitor compliance to Third Party risk or risk appetite?



All this risk information is getting reported to the board and risk committees, with almost 30% reported to the board annually. The next most common reporting times to the board were quarterly (18%) and ad hoc (18%). Almost one-third also noted that the executive risk committee gets quarterly reports and another 20% stated ad hoc reports to this committee.

How frequently does ERM or TPRM report on these risks:



Software

Several organizations were exploring or using software to help with TPRM. When asked if they use software to manage third-party risk, 37% stated they were using software and 19% were in the process of getting software. The risk leaders were also asked which software they use. One executive stated, "Multiple – primarily embedded in the core service system. We also leverage info/data security and vendor management internal systems." Others listed the actual software (Appendix 2 shows the software listed by the organizations that responded to the question).

Benefits of ERM Involvement with TPRM

In discussing the benefits of ERM involvement, one risk leader noted that ERM can add value by defining the risk landscape, by assisting with risk assessments, by analyzing residual risk analysis, and by helping with any due diligence questionnaires. Another noted that ERM can

benefit an organization by getting involved in the contracting process and the review/assessment process and then bringing in an enterprise level view of these risks. **ERM can also help by breaking down the silos and by helping to pull this into a central view (especially from a governance perspective).** Several risk leaders noted the importance of knowing who to get involved in governance of third-party risks (and who *not* to get involved).

All this effort is leading many organizations to determine if their efforts are bringing results. Around 14% stated that they are using Key Performance Indicators (KPIs) to track the effectiveness of their TPRM efforts. Revealing the amount of work happening in this area, another 42% stated that they are in the process of establishing KPIs. A few examples of the KPIs included the number of contract reviews completed and the likelihood of supplier risk getting reduced for critical suppliers. Others noted they were tracking the level of errors, incidents, timeliness, quality, and the level of compliance by third parties.

Building TPRM Case One

One organization shared their journey in building a third part risk management program. The risk leaders at this organization noted the strategic significance around their supply chain. Specifically, they noted that their company is undergoing transformation and that the supply chain is part of that transformation. They reiterated some ERM fundamentals to consider in this area including the need to coordinate the management of risks, the importance of a consistent risk approach, the need for harmony, and the significance of not having assurance gaps. This organization also explained that building TPRM was a multi-year journey, for them a journey that started with identification of third-party risk during a fraud risk assessment. From there they set up a steering committee, developed a project charter, benchmarked their program, engaged external stakeholders, launched a kick-off, and eventually implemented a TPRM program with policies, guidelines, resources, and training. This TPRM function provides central visibility into their third parties, a formal pre-contract inherent risk assessment and due diligence, use of standardized risk mitigating provisions, and risk-based monitoring and oversight.

The organization also discussed the future state of their TPRM, including third party qualification and approved bidder lists. They briefly explored the inherent risk assessment process and their twelve risk domains they use when doing their due diligence (including sample domains such as information security, fraud, business resilience, and reputation). The due diligence leads to the residual risk and third-party assessment, along with the eventual risk treatment. Another view of their future state included risk governance. This governance included key topics on escalation, reporting metrics, and a third-party risk committee that reports to the executive committee.

Building TPRM Case Two

Another organization presented their ERM and supply chain risk management program. This organization stated that their objective for ERM was to develop a holistic view of the most significant risks that could impact strategic objectives and they applied that view to supply chain and third party risks. **Their program had evolved from viewing supply chain as a risk to viewing supply chain risk management as a competitive advantage.** As part of their progress they established a supply chain center of excellence with a mission to "build a connected supply chain risk program to enable a resilient end-to-end value chain service to the business." They wanted to be risk aware and drive decisions (e.g., let the risk profile of the third party drive the mitigation actions).

They improved organizational preparedness by providing visibility with tools such as a supplier risk index, a material risk index, demand forecasts, and risk maps. The visibility and the additional integration helped them to improve their risk aware culture too. They also had annual processes related to critical suppliers, critical plants, and critical material in addition to weather alerts, response teams, and global supply chain maps. The tools were valuable and helped them leverage data for improved supplier resilience strategies (among other things). For example, the supplier risk index included metrics on the number of out of tolerance suppliers, the overall risk score by vendor, the financial health, and assessments (by vendor) on several

risk areas including responsible sourcing, cyber security, food safety, and an inherent country risk score. Additionally, their material risk index enabled them to see the "critical materials" (a combination of the highest risk and the highest impact) and is used to improve prioritization. Using this visibility and assessments, along with a performance playbook, they are able to build risk management into the processes to improve responses, manage exceptions, and act quickly (sometimes before the risk event occurs).

Risk Leader Insights

During the Summit the risk leaders split into groups to dig deeper and share their insights and concerns. The need to dig deep and to fully understand the nature of third-party and supply chain risk was mentioned many times. **One risk leader described third party risks as a spider web that you must unravel to understand.** The nature of the risk included understanding if the risk was physical or digital. It also included understanding who generates the risk; i.e, whether it is actually a third-party or a fourth or fifth party. Understanding the risk also means knowing if the risk is strategic, if it is related to critical assets or secrets, and how the risk impacts the organization's reputation. Some saw third-party risks as highly regulated but admit that the regulators approach may not be consistent with the business and strategic needs of their organization. Many admitted they needed to better align third-party risks with the ERM program.

To understand the risks some organizations conducted deep dives and were not always pleasantly surprised at the findings, even discovering that vendors were doing more outsourcing (with increased risk) than previously understood and were creating multiple layers of third-party risks. **A few organizations mentioned that until they did a deep dive on third-party risks, they simply did not know about potential risks and their impacts.** Further, they had no centralized knowledge of the risks before they began to dig into these risks.

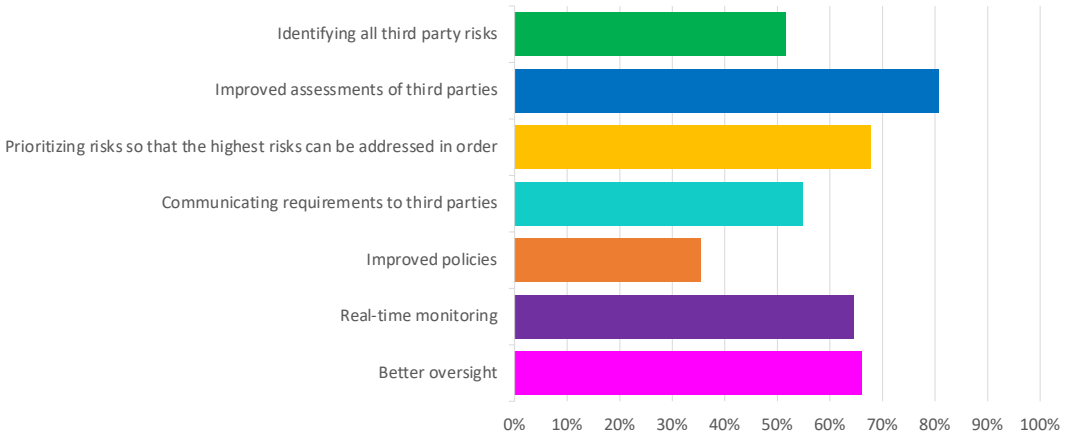
Many risk leaders noted that their approach to TPRM had been very traditional with either supply chain or procurement taking the lead. Many also noted that compliance and legal are

involved. Others noted, however, that this can miss the strategic and criticality of the risk around the supplier. One risk leader shared how they were identifying all 'critical suppliers' for their critical components. They added that they wanted to ensure that all critical suppliers had business continuity plans but admitted that even knowing that doesn't ensure that losses can be absorbed. ERM must drive these big questions. One risk leader reminded their breakout group, "ERM is not running a third-party program but we are there to remind them of what it is and how important it is."

Conclusion and the Keys to Improving TPRM

Everyone wants to improve their risk management and that includes third-party risks. Risk leaders were asked the areas to improve (see the full list of responses in Appendix 3) and several noted the importance of governance over the process while others mentioned the process itself. Related to the process were replies about the importance of embedding risk management, training, ownership, working with the business units, and being consistent or standardizing their approach. Others stated they were going to increase audit and enforcement. From a pure ERM perspective, there were many responses around risk identification and risk assessment. As noted in the case studies, improving TPRM is a journey. One key is to get started on building a TPRM program and linking it to ERM. Another key is to improve on the existing TPRM program.

The key to improving TPRM is: (Check all that apply.)



Appendix 1 – How Does TPRM Engage with ERM?

They are a top risk for ERM and develop risk drivers and mitigations which are reviewed at start of year and reviewed quarterly for emerging trends, present status of risk to LT and Risk committees
Risk Committees Risk Assessment Action plans
It is part of ERM
ERM is partnering with TPRM team to build out a program as a Steering member
Consistent interaction particularly around cybersecurity incidents whereby ERM group is trying to enforce and monitor company policies and procedures
Formal risk owner with defined risks, mitigations, and metrics. Additionally, engage on projects and initiatives to address emerging risks.
Alignment on taxonomy, criticality, and escalating key issues
Similar risk classification methodology.
TPRM is a function of our supply chain. Our executive supply chain member participates in on and represents TPRM in our executive risk council meetings

Although we have a federated approach, we've established centers of excellence to provide standard guidelines for everyone to follow. We are still working on defining a way to provide oversight across all the teams from an ERM point of view.
The TPRM function resides within the same Division (Enterprise Risk & Governance) as the ERM function, reporting to a single executive leader.
Opportunities exist in this area.
Management via the same team, with close collaboration on work plan and results.
TPRM consults with ERM to help drive alignment across business units and functions on third party risk management expectations. ERM also consults on overall process and framework.
TPRM is incorporated into the annual ERM Risk Map exercise.
TPRM sits under the ERM in our organization.
Provides input into the ERM process owned by Internal Audit
We currently don't TPRM - this was identified as an opportunity through ERM risk assessment. Op model for engagement is still TBD.
As normal input to the program like any other source
Supplier risk team engages with ERM in risk mitigation, monitoring and reporting activities.
Third Party is a single risk on our Enterprise Risk Register. However, we've aligned the TPRM risk register as L2 and L3 risks under the Enterprise Risk Register.
Submits formal RCSA annually and updates as beneficial/needed. Consults with ERM on new initiatives, significant business or vendor related change.
Work together on operational risk issues and policy setting
ERM = Strategic Risk Identification TPRM = Operational Execution of Risk Mgmt Program A close partnership across these teams is in place.
Supply chain and operations interdependencies are one of our 10 key risk areas with an assigned executive level risk owner who monitors developments and management programs which are reported to the ERM Steering Committee in rotation with other risks.
TPRM is in process. We meet regularly with key relationship owners to monitor specific third party risks.
Mostly IT focus and ERM engages on tools & techniques and metrics.

Regular interactions between ERM and TPRM. ERM works with TPRM to understand Risk Appetite Metrics
Identification of significant, unmitigated risks and escalation to ERM for risk acceptance/decision making
Risk interviews, risk sponsors, risk owners
It is integrated in all ERM level risks
Leverages ERM risk assessment framework to ensure consistency TPRM provides input in quarterly risk reporting
Integrated in terms of Risk Owner accountability, and interdependencies of business activities performed by TP with overall Business Objectives
ERM team has been charged with leading the implementation and operations of the SCRM program
Partnership between TPRM and ERM to enhance risk protocols; if TPRM is deemed a key risk then it might fold into ERM governance
Currently in development
ERM has continuous conversations with Global Procurement Finance and Global Security to ensure awareness and building of proper Business Continuity Plans
We have multiple departments who support TPRM and ERM/Compliance is involved in trying to coordinate those efforts more formally, including a specific third party risk assessment. We are also rolling out a GRC tool that will have a third party risk module.
Currently the TPRM program has not been established yet. ERM is a stakeholder in the development of the program.
We have an ERM unit; but, Third Party Risk Management is considered during the Procurement Process
SCRM is a sub-committee to the ERM committee

Appendix 2 – Responses to Which Software Is Used to Manage Third-Party Risk

Archer	Formstack	Resilinc
Ariba Risk	Risk Score	Interos
Share point	Fusion	Everstream
Confluence	Onspring	OneTrust
D&B	Securemate	Excel
CyberGRX	Resolver GRC	IRM
Metric Stream	SAP Ariba	

Appendix 3 – Top Areas to Improve TPRM in the next 12 Months

#1	#2	#3
Actively rolling out a more cohesive, centralized, risk-based, fit-for-purpose approach to TPRM	Actively managing third party risks through existing business processes (e.g., Cybersecurity, 5/4/2022 9:50 PM Privacy, IT Services, EHS, Quality, BCM, etc	Identify suppliers with elevated cybersecurity risk during sourcing process; continue to partner with cybersecurity on incident response
Real-time monitoring	On-site visits	Action plans to address gaps with accountability to close on time
Better Reporting	Stronger leadership within team	Establish resources to sustain program over next 3-5 years
Process enablement via technology (program roll-out)	Governance structure & reporting (including common taxonomy)	Enforcing adherence to the policies and procedures
Identification of third parties	Creating a coherent and applicable set of policies and procedures	Physical locations of 3rd party's resources
Supply Chain resiliency	Cybersecurity	Org change management
Establish criticality assessments	Onboard technology platform	More responsive procedures for handling vendor adverse events
Better software/systems to collect and assess risk levels	Improved monitoring (real time) for vendor risk	More forward and proactive monitoring, less reactive
Expand use of software	Consistent diligence across all businesses	Communicating/monitoring expected results
TPRM governance	Better organizational systems that guide focus areas	Contract pricing because of inflation
Identifying/prioritizing third party risks	Assessing third parties - handling/ needs of data	Ensuring tracking of red-lines or pushback from third-party vendors with

		established MSA terms and conditions
Supply Chain considerations	The Great Resignation impacts	Develop KRIs
Ensuring business units proactively consider use of vendors and engage TPRM	Consistency in monitoring (real-time) compliance with third-party obligations	Improving identification of the highest risks
Contract enforcement	Increased audit activity	Payments
Supply chain	Follow-up on issues identified through data analytics	Aligning more closely to established business process
Identifying all key third parties	Due diligence	Further embed monitoring
Data analytics	Streamlining the systems of record	Implement monitoring and metrics
Oversight	Further embed TPRM expectations across units/functions	Contract management
Imbedding a new management resource	Retroactively apply to vendor universe	Global centralized distribution of product
Supply chain	Oversight	BIA
Strengthen ownership and clarify roles/responsibilities	Clarifying the relationship between TPRM and ERM	Cyber risk
Complete formal process documentation	Sole sourcing of equipment and parts	Business reliability and resilience
Workflows	Contract risk review	Incorporating KPIs and KRIs
Assessing the right governance of TPRM	Better identifying and addressing bus change - internal & vendor initiated	Data privacy
Supply chain source of parts	Supplier Insolvency	Key risks (cyber and supply risks)
Tier n visibility	Training	Multi-sourcing
Increased monitoring	Quality compliance	Business unit TPRM
Maturing our TPRM monitoring program and related reporting	Switching software vendor	TPRM Resiliency and Agility

Supply Disruptions	Cybersecurity	BU focus on 3rd party risk management
Process / System improvements	Process	Update our SCRM strategy
Regulatory compliance	Monitoring changes in third party scope/risk profile	Include vendor risk in ERM to identify additional actions
Tighter coordination with Supply Chain	Supply tracking	Monitoring
Reassessing Essential and Critical Suppliers	Adherence to service level agreements	Improve auditing of third parties
Automated vendor screening	ESG	Formalize process to onboard / approve third parties
Governance	TPRM Crisis Management	
Establishing KRIs	Improved ERP system	
Contracts	Expand involvement beyond ERM and Cyber teams	
Contract reviews	Perform audits	
Faster	Improve due diligence related to information security requirements	
TPRM cybersecurity exposure	Process Implementation	
Enhanced policies	Coordinate IT security review with business level SLA monitoring	
Tailoring the monitoring of vendors – moving away from the current one size fits all approach	Establishing risk ranking questionnaire	
Expansion of the TPRM program		
Defining roles and responsibilities for oversight		
Developing a standard		
Update risk assessment process		
Identifying and rationalizing inventory of third parties		

Center for Excellence in ERM Advisory Board

Dr. Paul Walker Schiro/Zurich Chair Enterprise Risk Management Director, Center for Excellence in ERM, St. John's University	**John Adams** Retired VP Global Enterprise Risk Management, PepsiCo
Kimberly Chacko Senior Consultant, Risk and Compliance, Protiviti	**Russ Charlton** Chief Audit Executive, Advance
Blake Eisenhart Retired Chief Audit Executive, Unisys	**Geralyn Fanelli** Global Enterprise Risk Management Sr. Director, PepsiCo
Stuart Horn Director of Enterprise Risk Management, IBM	**Deon Minnaar** US Lead for Board Advisory Services, KPMG
Adrian Mueller Director of Enterprise Risk Management, MasterCard	**Rich Muzikar** Enterprise Risk Management Advisor, Long Island Power Authority
Matthew Perconte Managing Director, Protiviti	**Steve Richard** Senior Vice President, Chief Risk Officer, Becton Dickinson & Co
Chris Ruggeri National Managing Principal Risk and Financial Advisory, Deloitte	**Rob Ryan** Partner, PWC
Kelli Santia Risk Manager, Strategic Risk Management, General Motors	**Denise Sobczak** Director Enterprise Risk Management (ERM) – BIC Group
Jorge Tercero Global Enterprise Risk Management Sr. Director, PepsiCo	**Zach Wolff** Director of SOX & Enterprise Risk Management, Con Edison
Arya Yarpezeshkan Chief Risk Officer, Global Specialty, AIG	**Mei Young** Executive Director, Enterprise Risk Management, Estee Lauder Companies Inc.