Third-Party Risk Management:

Trends and Strategies to Help You Stay Ahead of the Curve

AUDITBOARD

RSM

Table of Contents

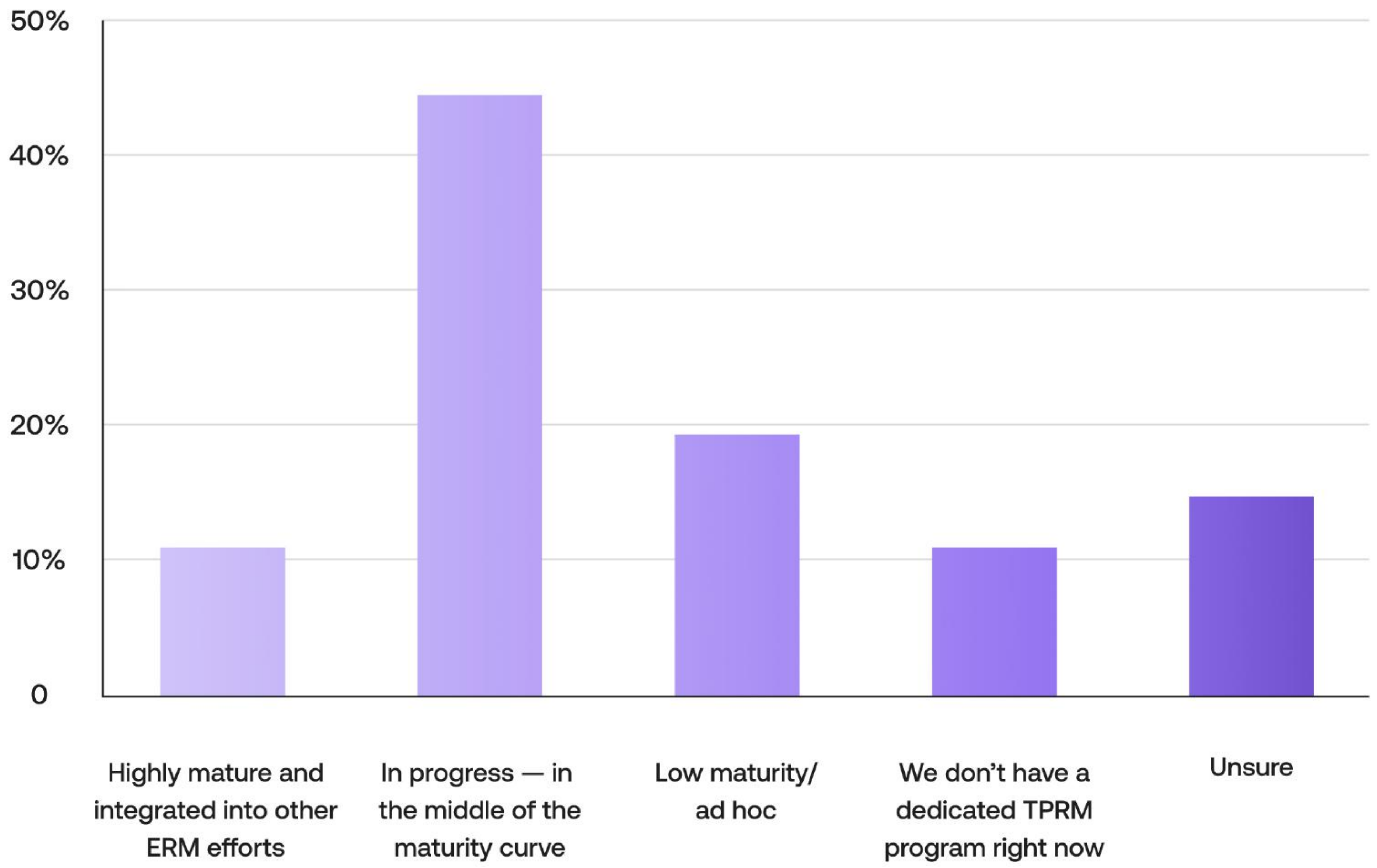
Introduction

The use of third parties for critical business functions has grown exponentially in recent years. A trend that was started as companies began to embrace digital transformation spiked during the pandemic and shows no signs of abating. While leveraging third-party suppliers, vendors, partners, or software providers for core functions can offer efficiencies, cost savings, and other benefits, it also exposes companies to a variety of risks (see Figure 1). Unfortunately, most companies are still struggling to mature their third-party risk management (TPRM) programs, leaving them vulnerable — unaware of the risk they've taken on, and unprepared to respond in the event of an incident.

Many businesses learn this the hard way: 59% of organizations surveyed in CrowdStrike's *2022 Global Threat Report* didn't have a response strategy in place when they suffered their first software supply chain attack. CrowdStrike's report also found that while 84% of respondents believed supply chain attacks could become "really significant" over the next three years, only 36% had vetted all new and existing suppliers in the past year. Recent breaches such as LastPass are impacting public companies that are now required to take action on these types of supply chain breaches.

A 2023 AuditBoard poll of 1,000+ internal audit and risk leaders showed a similar disconnect. While more than 50% of respondents reported increasing their use of (and reliance upon) third parties since 2020, only 12% rated their organizations' TPRM program maturity as "highly mature and integrated into other ERM efforts." More than 11% didn't have a dedicated TPRM program, 19% reported low maturity, 11% were "unsure" of maturity, and 44% were "in progress — in the middle of the maturity curve."

How would you describe the maturity of your third-party risk management (TPRM) program?



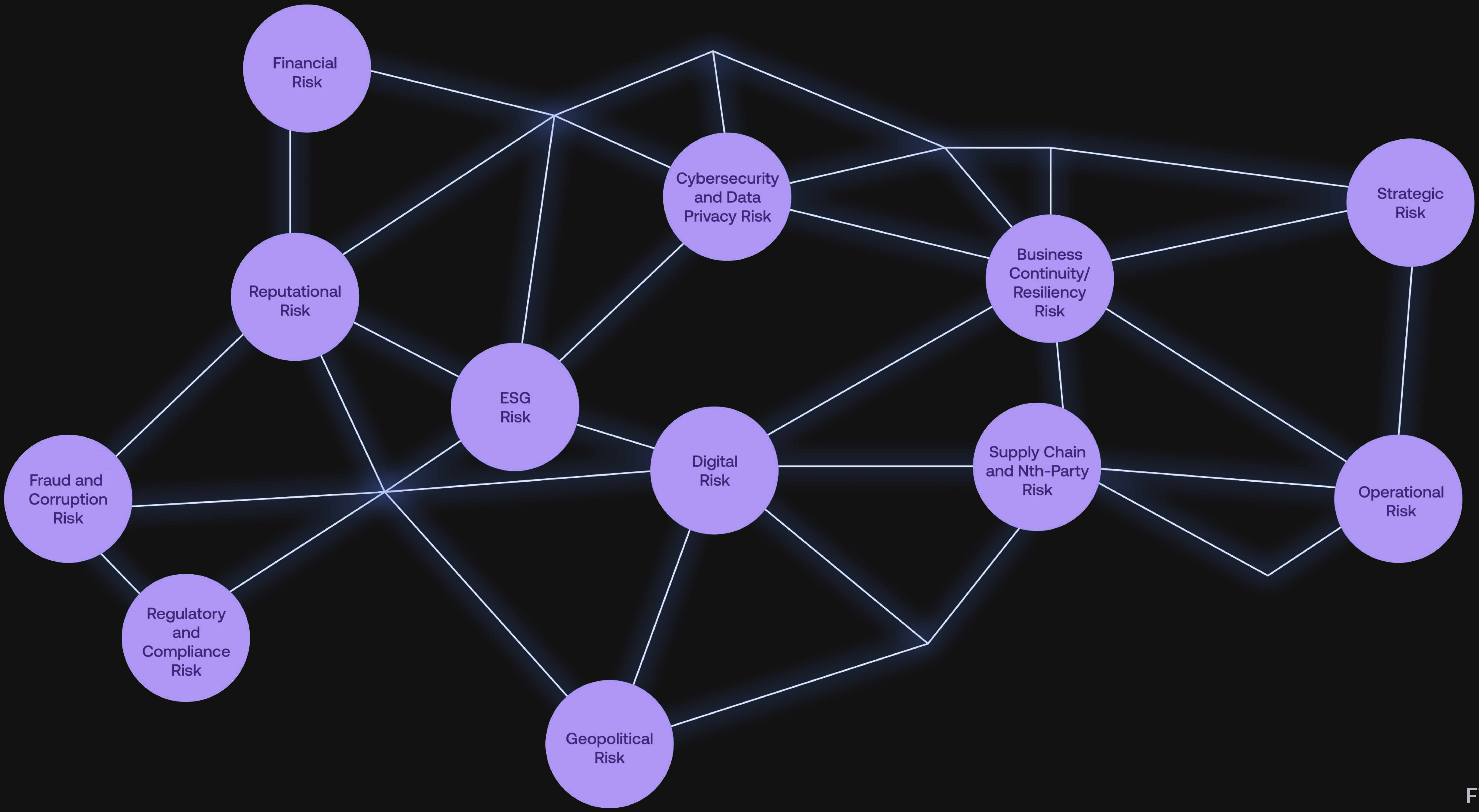

Financial Risk
Cybersecurity and Data Privacy Risk
Strategic Risk
Reputational Risk
Business Continuity/ Resiliency Risk
ESG Risk
Digital Risk
Supply Chain and Nth-Party Risk
Operational Risk
Fraud and Corruption Risk
Regulatory and Compliance Risk
Geopolitical Risk

Figure 1

The reality for most businesses is that third-party risk is only one challenge among many. In today's volatile risk environment, new risks emerge at ever greater velocity as businesses continue grappling with heightened existing risk in areas such as data, cloud, and remote workforce technology security; talent management; legislative and regulatory compliance (e.g., cybersecurity, personal data privacy, climate and sustainability); and supply chain management. These same businesses simultaneously face continuing economic uncertainty, resource constraints, and budget pressures.

As recent TPRM trends show, however, many businesses are nonetheless prioritizing efforts to mature their TPRM programs. Executive focus is increasing rapidly, driving the need for better and more actionable data. Companies know they need to better understand the risk they're taking on relative to their use of third parties and third-party software. **The time is now to assess TPRM maturity and improve how your organization prioritizes, monitors, and responds to third-party risk**. Our guide breaks down the trends to offer strategies and best practices to help your company stay ahead of the far-reaching third-party risks on the horizon.

The Third-Party Risk Management Life Cycle

TPRM is a cyclical process of identifying, evaluating, mitigating, and monitoring the risk presented to your organization by the third parties you engage. By assessing the risks presented by each third party, you can determine if and how the risks can be accepted, transferred, or mitigated.

It's important not only to understand the risks in advance of engaging a third party, but also to continuously monitor risk as it evolves throughout the relationship. Risk is dynamic, changing over time, such that categorization, assessment, issue management, reporting, and continuous monitoring must be periodically revisited. That's why TPRM should be embedded at every stage of the third-party life cycle, from sourcing and due diligence through contracting and onboarding, ongoing monitoring, termination, and offboarding. AuditBoard's *Effective Third-Party Risk Management: Key Tactics and Success Factors* offers key principles and tactics for maturing TPRM programs.

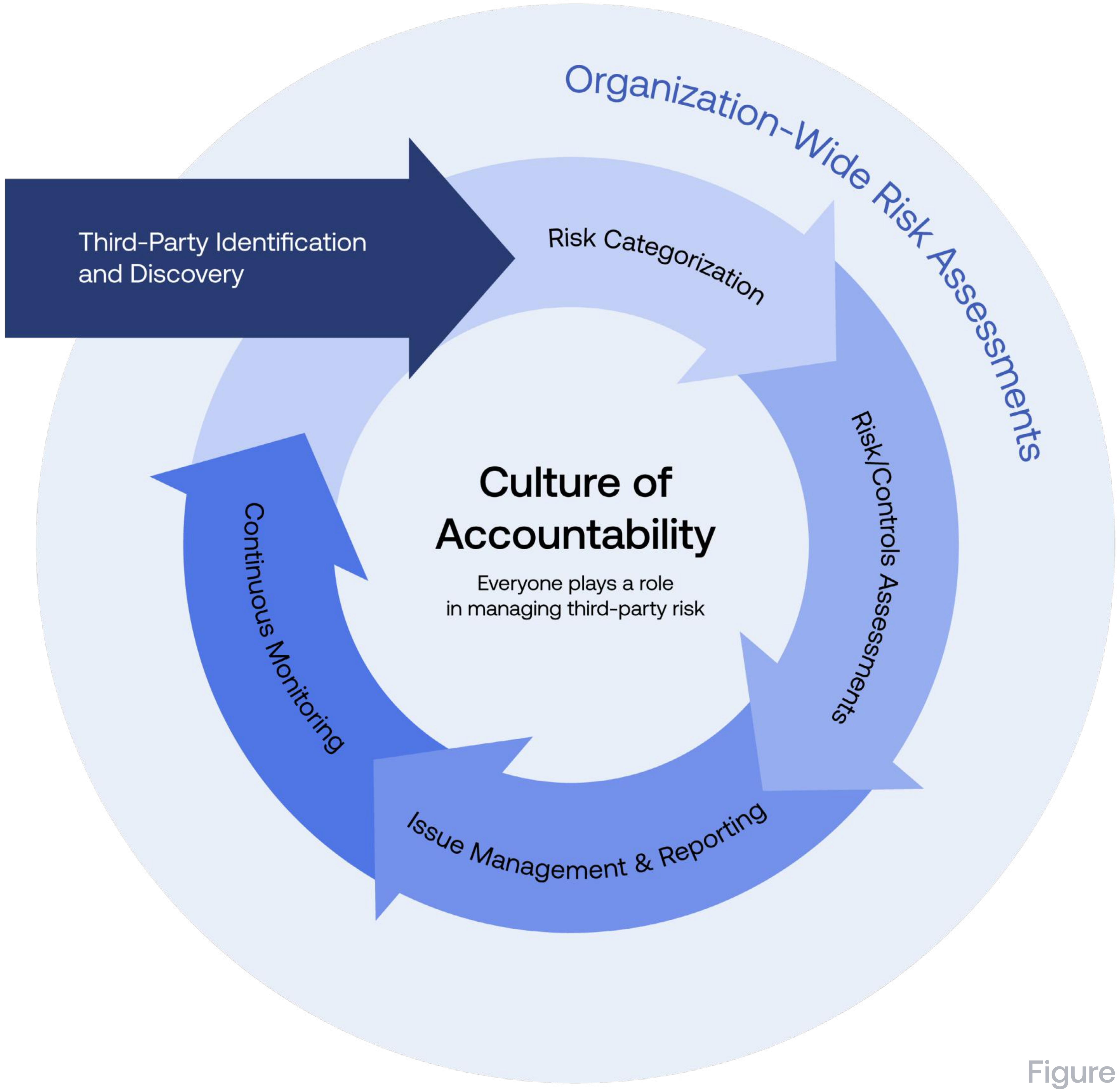

Organization-Wide Risk Assessments
Third-Party Identification and Discovery
Risk Categorization
Risk/Controls Assessments
Issue Management & Reporting
Continuous Monitoring
Culture of Accountability
Everyone plays a role in managing third-party risk

Figure 2

TPRM Trends on the Horizon

RSM provides TPRM maturity assessment, internal audit, program build/design, and technology enablement services to companies across a variety of industries. In looking at how and why clients engage RSM and what they're experiencing, we've noted several recent trends. These trends yield insight on the evolving third-party risk landscape and how companies are successfully using TPRM to respond — and can translate into strategies to help you mature your own TPRM program.

TPRM Governance and Oversight Trends

Elevated Focus From Leadership

Given the continued escalation of third-party cybersecurity breaches and enforcement and supervisory authority scrutiny, boards, audit committees, and C-Suite leaders are asking more questions about TPRM than ever before. They're also interested in **using TPRM data to benefit the organization** and improve how it manages third-party risk. As leadership focus increases, so does **the need for timely, accurate, and meaningful TPRM information**.

Heightened third-party risk, coupled with an elevated focus from leadership, is transforming how companies think about TPRM. Instead of contemplating it as a simple inventory or a point-in-time assessment, the **shifting mindset** requires viewing TPRM through a lens of **how companies rely on third parties for key business processes that are critical to operations** and **continuous monitoring** throughout the third-party life cycle. What is procured from each third party, and how do the goods or services impact critical business processes? How resilient is the organization around any critical processes supported by third parties?

This shift in mindset is positioning companies to **use TPRM data in new way**s. For example, they may use TPRM data as an evaluating factor to make business decisions relative to who they're engaging with on critical functions. It can also reveal opportunities to consolidate service providers or get more favorable terms and conditions (T&Cs) based on utilization.

Increased Centralization, Integration, and Consistency

Historically, supply chain risk sat with logistics and operations, with decentralized risk management conducted by departments or other internal silos performing their own due diligence. However, **in decentralized models, the left hand doesn't always know what the right hand is doing, leading to inefficient, inconsistent practices for identifying and assessing risk**. In addition, many organizations may not have workflows to create or respond to questionnaires focused on vetting third parties, performing these duties on an ad hoc basis that lacks efficiency or consistency. Lastly, third-party contract T&Cs tend to vary widely, creating disparities in how departments interact with third parties across the organization and at times can create bottlenecks as legal departments review varying T&Cs.

Current trends show organizations working toward centralization and integration that supports more standardized processes and workflows. Specifically:

- We're seeing a push toward **more integrated TPRM models**, where everyone is involved in one enterprise-wide process, and a central group oversees procurement and/or sourcing. Hybrid models — in which a central procurement function oversees TPRM but may give groups leeway to procure as they need to — can be a fit for some organizations.
- Many organizations' baseline due diligence reviews rely on **standardized questionnaires based on vendor type**, in addition to any SOC reports or industry-specific certifications.
- Organizations are moving toward **more consistency in the T&Cs** used in third-party contracts.
- Distributed TPRM responsibilities (e.g., legal, compliance, internal audit, procurement, IT) are creating the **need for workflow tools** to help organizations standardize and streamline processes.

TPRM Technology Trends

The increase in TPRM questionnaires and need for greater integration/centralization — paired with the heightened focus from leadership and ongoing resource constraints — are driving a trend toward **increased utilization of technology tools** for driving and managing TPRM activities. This trend is also being accelerated by the **elevated interest in using automation and AI-powered risk intelligence**. Businesses want to be able to efficiently mine third-party data to **identify and understand key third-party risks and uncover enhanced insights** that can be used in contract negotiations or renewals. They also want to be able to **react and comply efficiently with any changes in reporting requirements** relative to third parties. See "Regulatory and Compliance Risk Focus" on page 13 to learn more.

Responding to this growing appetite for enabling technologies, AuditBoard's TPRM solution supports organizations in inventorying, screening, categorizing, and monitoring third-party relationships and risks, streamlining workflows, and automating many TPRM program features.

TPRM Risk Focus Trends

Every company faces an enormous array of third-party risks. Figure 3 gives an overview of the major categories. In our experience, the risks shown in purple are receiving heightened focus in the current environment. We'll take a closer look at each risk below.

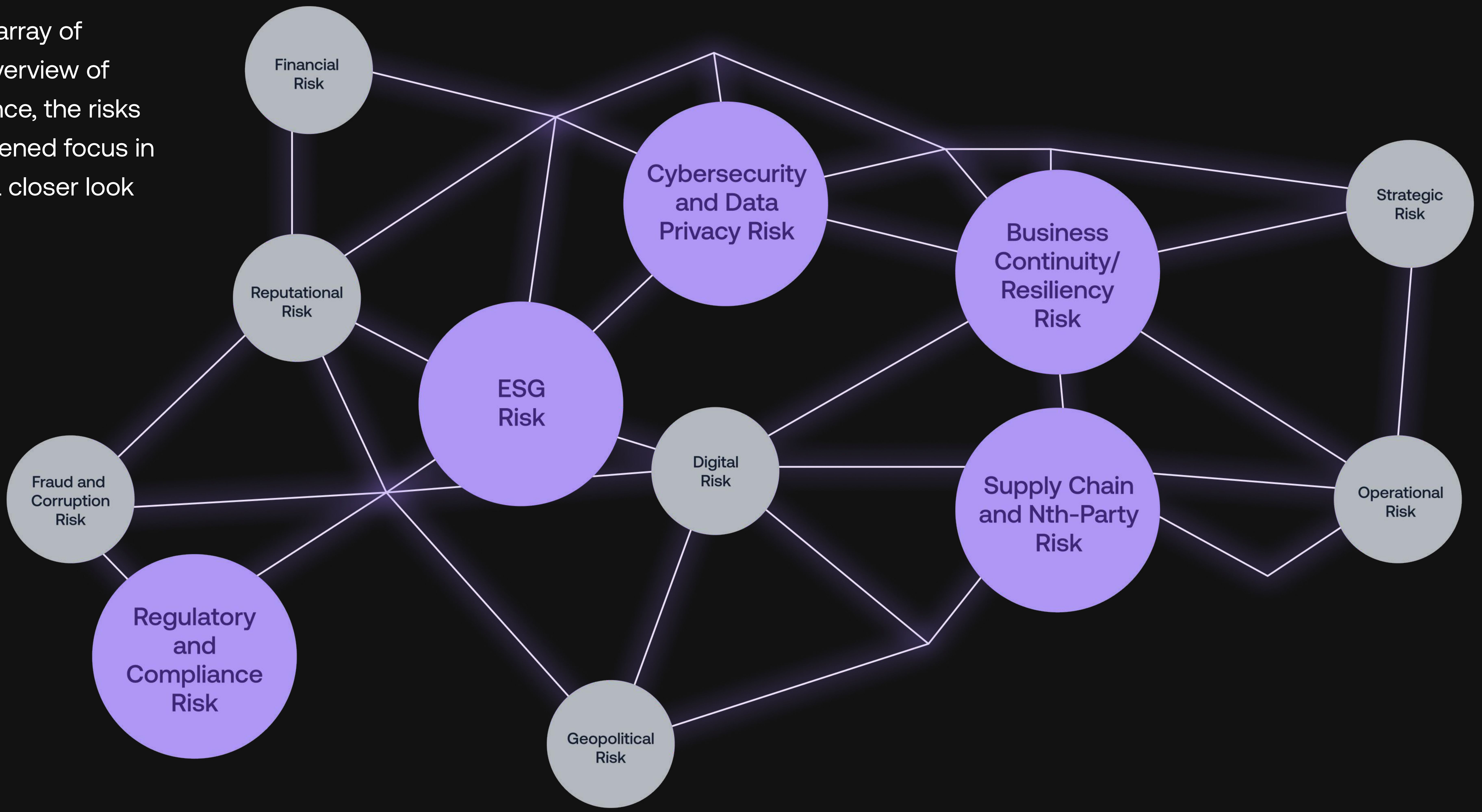

Financial Risk
Cybersecurity and Data Privacy Risk
Strategic Risk
Business Continuity/ Resiliency Risk
Reputational Risk
ESG Risk
Digital Risk
Supply Chain and Nth-Party Risk
Operational Risk
Fraud and Corruption Risk
Regulatory and Compliance Risk
Geopolitical Risk

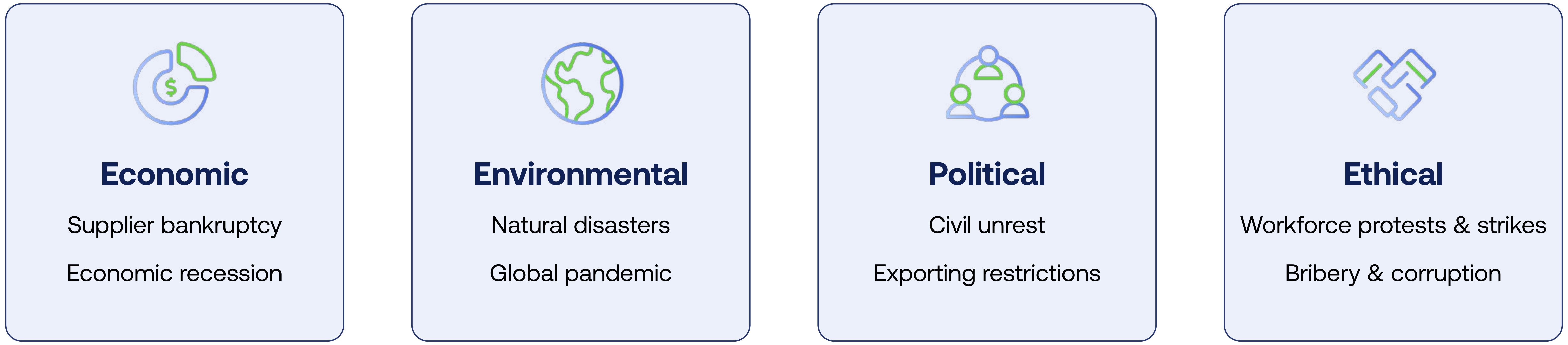
Figure 3

Supply Chain and Nth-Party Risk Focus

Your company's supply chain comprises the flow of goods and services made up of internal and external third parties, including any software supporting those goods and services. Today's volatile risk landscape requires us to look beyond third-party vendors to include *their* vendors and beyond. This is called **Nth-party diligence**, and it involves understanding how data is transferred from your organization to each third party and their Nth parties.

Prior to the COVID-19 pandemic, supply chain risk was an afterthought for many companies. Now, **supply chain issues often change how companies do business**. The **supply chain often leaves companies more vulnerable**, and these vulnerabilities will not go away. Figure 4 depicts some of the most prominent supply chain risk trends and focus areas.

In response to these vulnerabilities, **regulators and standard-setters are issuing guidance** encouraging companies to adopt key practices to better manage Nth-party risk. For example, new guidance from the National Institute of Standards and Technology (NIST) focuses on helping companies build cybersecurity supply chain risk considerations and requirements into their procurement processes. NIST reinforces that it's more important than ever **to plan for supply chain issues** and **use due diligence, risk assessments, and reviews to understand who critical vendors are**, how they impact critical business processes, what their business continuity and disaster recovery processes entail, who their Nth parties are, and how they perform diligence around them.



Economic
Supplier bankruptcy
Economic recession

Environmental
Natural disasters
Global pandemic

Political
Civil unrest
Exporting restrictions

Ethical
Workforce protests & strikes
Bribery & corruption

Figure 4

Regulatory and Compliance Risk Focus

Emerging regulatory guidance and considerations are a key driver behind the momentum for maturing TPRM programs. It's worth noting, however, that the regulatory activities are in turn being driven by increasing risks and costs in all of these areas, as well as a cultural shift marked by greater focus on supplier transparency. In particular, the regulatory and compliance focus areas below are quickly growing in prominence.

- *CYBERSECURITY*

The **U.S. Securities and Exchange Commission (SEC)** is continuing to release **cybersecurity disclosure rules** for public companies. The proposed rules require immediate disclosure of material cybersecurity incidents and **annual disclosure of cybersecurity risk management policies and procedures** (including management's role in Third Party Risk Management), the board's level of cybersecurity risk management oversight and experience, previously undisclosed immaterial incidents that have become material, and updates on previously reported incidents.

The **U.S. Department of Labor (DOL)** has announced new cybersecurity guidance for plan sponsors and fiduciaries regulated by the Employee Retirement Income Security Act (ERISA). The guidance offers a range of cybersecurity program best practices, notably including a **"reliable annual third-party audit of security controls"** and **"appropriate security reviews and independent security assessments"** of "assets or data stored in a cloud or managed by a third-party service provider."

Other U.S. government bodies are simultaneously formulating legislation and guidance to help companies better prepare for and defend against cyber attacks. For example, the **Cybersecurity & Infrastructure Security Agency (CISA), Cyber Safety Review Board (CSRB),** and **U.S. Senate** are each working on related guidance on enhanced vendor supply chain risk assessments and disclosure protocols.

- *NTH-PARTY DILIGENCE*

The **Office of the Comptroller of the Currency (OCC)** has issued interagency guidance asking banking organizations to take a broader focus on risk. The guidance would apply to "any business arrangement between a banking organization and another entity, by contract or otherwise." Notably, it goes beyond credit, operational, and reputational risk to **cover a much wider range of criteria across the entire third-party life cycle**. It also considers fourth- and fifth-party risk (e.g., vendors, subcontractors, individuals).

- *PERSONAL DATA PRIVACY*

The General Data Protection Regulation (GDPR), which went into effect in 2018, was a bellwether moment for privacy requirements. Worldwide, United Nations survey data shows that 71% of countries have already **enacted privacy and personal data protection laws and regulations**; another 9% are in the process of drafting it. Six U.S. states

— California, Colorado, Connecticut, Iowa, Utah, and Virginia — have enacted comprehensive privacy and personal data protection laws and regulations, while other states have enacted privacy laws focused on certain personal data types such as the healthcare industry, financial services, and special categories of personal data such as children, along with privacy requirements targeted at data brokers, internet service providers, and technology platforms such as smart device app stores including the apps available in the marketplace. In other words, chances are that personal data privacy laws and regulations already apply to your business at some level, so it's imperative to **understand what personal data you're receiving from and/or providing to third parties relative to your personal data holdings for both corporate (i.e., human resources management) and commercial (i.e., revenue-driven) operations**. Visibility and oversight of your personal data holdings are the foundation to understanding whether you're in compliance with the different privacy requirements on a global scale. If your third parties have access to your personal data holdings, then you need to ensure they have controls in place along with operational practices to manage the extent to which that personal data is meeting with your compliance obligations

- *ENVIRONMENTAL, SOCIAL, AND GOVERNANCE (ESG)*

Regulatory activity and investor pressure focused on ESG reporting continues to escalate both nationally and globally. The UK and EU have already adopted proposals mandating ESG reporting, and the SEC's mandatory climate disclosure rule and the IFRS Foundation's International Sustainability Standards Board's (ISSB) voluntary standards are pending. Many companies **lack preparedness and maturity around ESG metrics, initiatives, and reporting, especially as it relates to climate and environmental considerations**. Nearly 16% of respondents in a 2022 AuditBoard poll of over 1000 compliance, risk, and audit leaders reported being "not prepared at all" to assess the ESG concerns of their third-party and Nth-party suppliers, more than 40% indicated that they were only prepared to follow minimum guidelines, and more than 35% said they didn't know how prepared they were.

Companies should note that the SEC climate rule is expected to extend beyond a company's own ESG reporting, with **provisions that may require companies to measure and track third-party emissions along a company's entire value chain** (known as "Scope 3"). The ISSB has confirmed that its standards will include Scope 3 reporting. In addition, ESG requirements will reach beyond climate- and sustainability-related disclosures to areas such as board oversight and other matters of corporate governance. As companies strive to manage third-party risk, they're **asking more questions about the social and governance issues** listed in Figure 5. We've seen companies starting to use these types of questions on requests for proposals (RFPs) and vendor due diligence questionnaires, **weighing ESG responses as evaluating factors in third-party selection or utilization**.

Environmental	• Hazardous waste • Carbon footprint • Toxic emissions and greenhouse gas emissions • Water consumption • Opportunities in renewable energy & clean energy
Social	• Diversity and inclusion • Human rights and social responsibility • Employee benefits, wages/pay equality • Values in vendor/supplier relationships
Governance	• Risk management and risk oversight • Organizational structure (board structure & tenure, CEO tenure) • Executive compensation • Political donations, anti-bribery policies, anti-corruption policies • Product safety & quality

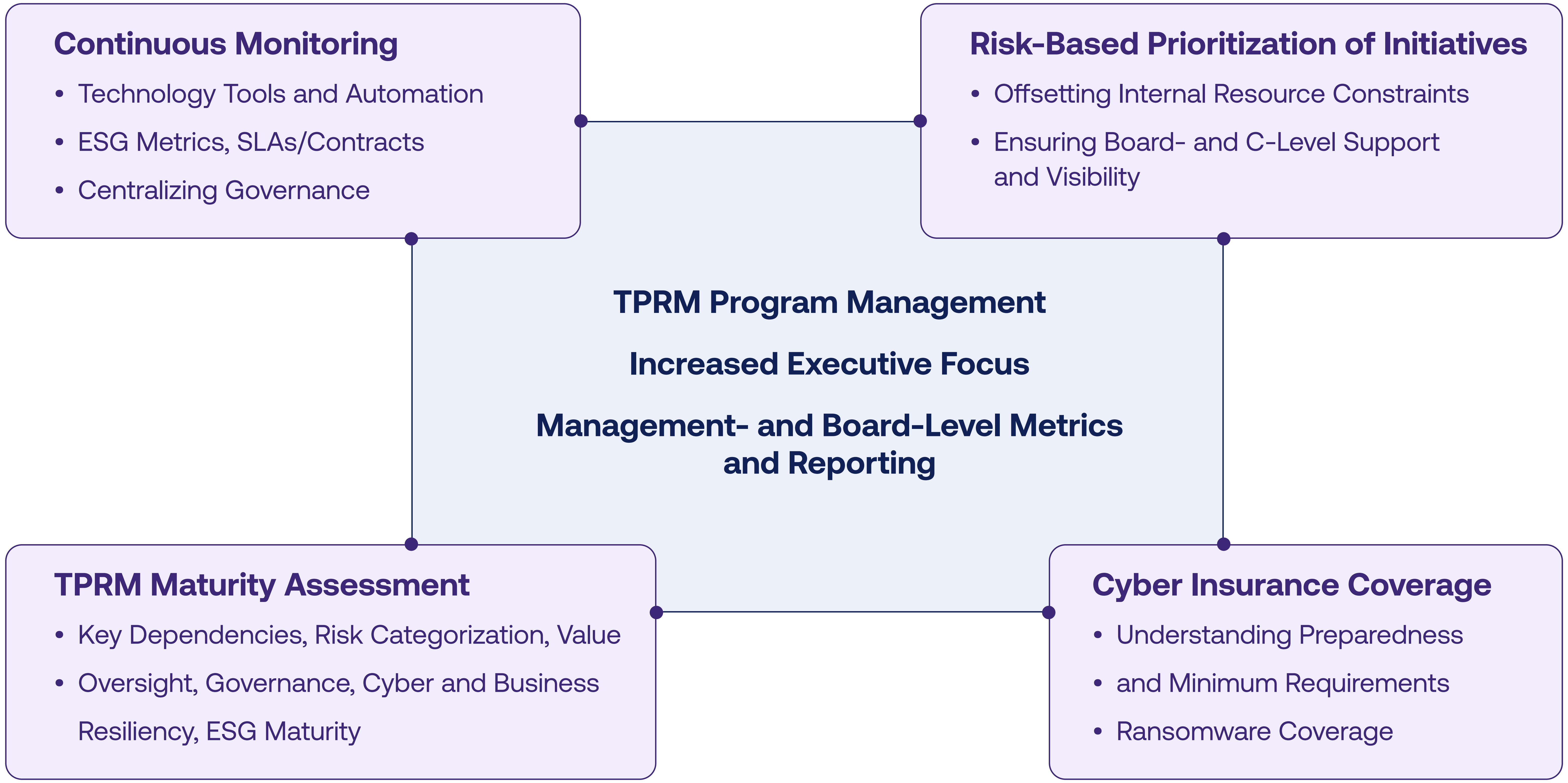
Figure 5

How to Stay Ahead of the Curve on TPRM

Recent TPRM trends tell us a great deal about where regulators and executives are placing their focus and how companies are responding. We can draw from these trends to create actionable strategies to help your company stay ahead of the third-party risk looming on the horizon and beyond.

Figure 6 offers an overview of the key TPRM initiatives we recommend prioritizing. The following sections provide additional background, as well as detailed tactics to help you get started.

Figure 6



Continuous Monitoring

- Technology Tools and Automation
- ESG Metrics, SLAs/Contracts
- Centralizing Governance

Risk-Based Prioritization of Initiatives

- Offsetting Internal Resource Constraints
- Ensuring Board- and C-Level Support and Visibility

TPRM Program Management

Increased Executive Focus

Management- and Board-Level Metrics and Reporting

TPRM Maturity Assessment

- Key Dependencies, Risk Categorization, Value
- Oversight, Governance, Cyber and Business Resiliency, ESG Maturity

Cyber Insurance Coverage

- Understanding Preparedness
- and Minimum Requirements
- Ransomware Coverage

1. Increase Executive- and Board-Level Involvement

Recent trends reflect the reality that increased executive-level involvement and sponsorship is central to the success of any TPRM initiative. The elevated focus from C-suite executives, boards, and audit committees requires management to be ready to provide enhanced TPRM insights, including:

- Identifying **key risks in business processes** supported or owned by third parties (i.e., identifying key vendors critical to operations, resiliency around critical processes).
- Providing **third-party relationship insight** that can be utilized during contract negotiation/renewal (e.g., dollars spent, adherence to SLAs, performance to budget).
- Providing clear, relevant, forward-looking **executive-level TPRM metrics and reporting** (e.g., # of vendors, volume of data stored or processed by vendors, critical business processes dependent on key vendors, # of key control gaps identified, frequency of review, other KPIs built around TPRM processes) supported by processes and technologies that enable continuous monitoring.
- Providing information that helps the organization to react to and comply with **changes in reporting requirements** (e.g., cybersecurity and climate disclosure requirements).
- Gaining **assurance on the operating effectiveness of the TPRM program** (e.g., are controls working as designed; are policies and processes being adhered to) through internal audit risk and compliance assessments designed to test effectiveness.

Need help?

The 2022 RSM US Middle Market Business Index Supply Chain Special Report offers business leaders forward-looking insight and analysis of how supply chain disruptions are impacting companies and the actions they're taking to respond.

2. Prioritize TPRM Initiatives Based on Risk

As new risk areas emerge (e.g., banking disruptions, ESG, new regulations, etc.), our risk teams aren't typically expanding at the same pace to handle the increasing depth and breadth of exposure. We're typically addressing more risks with the same, or fewer, resources. A key way to offset internal resource constraints is by **prioritizing TPRM initiatives based on the level of risk**. We recommend **adopting risk management technology that supports effective prioritization** and lets you focus efforts on the third parties that will have the greatest impact — and likelihood of impact — to the organization.

To support effective prioritization and gain needed leadership support, it will be crucial to ensure board- and C-Level support and visibility through TPRM metrics and reporting. **Implementing data-driven metrics that visualize the risk landscape for your organization's third-party ecosystem will make stronger cases for new or increased investments** while showcasing value and risk-reduction to the organization. Consider metrics such as potential loss to your organization due to a vendor breach, annual vendor spend and cost-savings through vendor consolidation, risk mitigation rates, and service satisfaction rates to the business.

3. Enable Continuous Monitoring

Continuous monitoring is critical for effective TPRM in today's chaotic risk environment, in which risks emerge and change with increasing velocity and volatility. Unfortunately, in RSM's assessments, **continuous monitoring is often the least mature area of TPRM process** for many companies. Many companies still need to learn that continuous monitoring should look beyond issue management (e.g., responding to third-party cyber breaches or data leaks) to include monitoring of third-party service-level agreements, performance reviews, contract management, ESG metrics, and risk mitigation activities, as well as appropriate rediscovery of inherent risks and reassessment of residual risks to evaluate whether anything has changed with third-party risk levels, categorization, and prioritization. Continuous monitoring should include providing timely alerts and insights to the business to stay ahead of third-party risk.

Incorporating questions from your due diligence assessments into your RFP and/or sourcing processes can identify risks earlier in the process, eliminating prolonged remediation windows throughout the contract duration. Early evaluation can also eliminate redundancy for your vendors and your internal teams, ultimately reducing internal costs while still aligning to your company's internal risk appetite.

Continuous monitoring can also strengthen the relationship between the third party and your organization. By establishing clear expectations up front and defining a regular cadence for follow-up, the third party is also provided with a clear path for open and transparent communication. **Ongoing evaluation allows for more timely risk identification** and gives the third party an opportunity to mitigate risk through proactive measures before they may escalate into larger risks or challenges. These check-ins can also be used to evaluate third-party performance, which may lead to fewer disruptions to product distribution and increased quality of service.

Many companies are **embracing TPRM technology tools and automation to help centralize governance** while supporting and automating continuous monitoring activities and workflows. These technologies can use TPRM data (including key risk indicators, or KRIs) to create strategic value for the organization and **drive continuous risk reduction across the third-party surface area**, whether through discovering new issues and propelling accountability for them or supporting TPRM reporting and remediation activities.

4. Consider Cyber Insurance Coverage

Every business faces third-party cybersecurity risk. Given the fast-growing financial, operational, and reputational costs of cybersecurity breaches, **cyber insurance coverage is quickly becoming a must-have for many businesses**, offering invaluable protection and assistance for helping organizations to withstand and recover from attacks. Unfortunately, we're in a **difficult environment for buying cyber insurance**, given ongoing breaches and ransomware incidents, the number of claims that have been paid, and the overwhelming risk insurers have taken on. Policies can be expensive, difficult to obtain, and replete with exclusions. For instance, in some cases we're seeing insurance carriers decreasing coverage rather than raising fees — if the previous policy had first-party and third-party liability, it may have only first-party liability today.

Cyber insurance is nevertheless an option for businesses looking to reduce their third-party cybersecurity risk. That's why we recommend **considering cyber insurance coverage**, and revisiting your coverage annually, weighing the costs and benefits for your company. In particular, make sure you understand the minimum preparedness requirements stipulated within the policies and within your underwriting application. Companies must ensure ongoing adherence to requirements for claims to be paid, which often includes questions regarding the organization's management of third-party risks.

5. Assess TPRM Maturity

Understanding the maturity of your TPRM program is foundational for reducing risk and moving towards a more secure program. The key considerations below can help ensure that you're asking all the right questions.

Understand Third-Party Dependencies, Categorization, and Value

Consider third parties' key dependencies, risk categorization, and value to the organization. **Identify critical vendors and assess their business and cyber resiliency.**

● *KEY CONSIDERATIONS*

- Remember, all third parties aren't equal. Determine the risk-criticality of third-party relationships by better understanding services provided, and the impact a loss of services would have to your organization. Put activities in place to mitigate risks to a level that is tolerable to your company's risk appetite.
- Different tiers deserve different review processes. Critical vendors need deep-dive reviews, and potential onsite audits, but a more narrow-scoped questionnaire may be sufficient for others.
- Focus assessments on the risk scenarios that matter for your organization, referencing the key risks identified via your existing enterprise risk assessment processes.

Need help?

AuditBoard's *Effective Third-Party Risk Management: Key Tactics and Success Factors* provides guidance on stratifying third parties in proportion to risk level and includes how-to information and pros/cons for a range of assessment tactics.

Assess Governance, Oversight, and Resiliency

It's critical to have a clear understanding of where you are to create a roadmap that can get you where you need to go. **Assess your organization's TPRM governance and oversight against leading practices**. The considerations below, while not exhaustive, reflect lessons learned from recent trends.

● *KEY CONSIDERATIONS*

- Consider connecting TPRM in with your organization's broader enterprise risk assessment process or cybersecurity assessment process.
- Weigh centralized or hybrid management of third parties to ensure more consistent, streamlined, and integrated processes and workflows. Consider outsourced managed services to assist with portions of the program where your company may not have internal resources with the skillset or capacity to support.

- Establish processes (e.g., training, top-down/bottom-up communications) that help to create a culture in which everyone is accountable for TPRM. Third-party risks are a team sport that should be played by all key players across the organization.
- Get a process/workflow in place to address questionnaires efficiently.
- Use standard questionnaires for third party completion, allowing for a more streamlined response timeline.
  - Ask about the use of Nth parties during the RFP/sourcing process to gain insight on any Nth-party services third parties are relying on.
  - Request and evaluate SOC reports to capture information about third- and Nth-party control environments and exposures.
- Consider enabling technologies to automate parts of your program and streamline workflows while increasing efficiency, productivity, and consistency.
- Adopt more consistent practices related to contracting and other processes throughout the TPRM life cycle. In particular, consider:
  - Using appropriate and consistent T&Cs in contracts for different categories of third parties.
  - Establishing baseline reviews for different categories.
  - Including a “right to audit” clause in contracts that allows you to check compliance with T&Cs via periodic audits.
  - Regularly updating contracts to reflect the latest regulations (e.g., personal data privacy, cybersecurity, ESG) and clearly delineating responsibilities between the parties.
  - Understanding whether third parties subcontract any of their obligations and whether third-party contract T&Cs flow through to the Nth parties.
- Stress test your TPRM strategy to identify and address vulnerabilities. Building a partnership with your internal audit team is another great way of ensuring ongoing improvement from an independent department.

Need help?

RSM’s article on “5 things to know about managing third-party relationship risks” provides more detailed background and guidance on these strategies and other aspects of TPRM.

Embed ESG Maturity and Preparedness Initiatives

Make sure your TPRM program **embeds relevant ESG maturity and preparedness initiatives** into third-party considerations and continuous monitoring. While needs will vary depending on your business model, industry, and location, the example TPRM initiatives below should help you get thinking in the right direction.

Need help?

AuditBoard's Step-by-Step Guide to Building Your ESG Program: Resources, Best Practices, and Key Considerations provides guidance around translating ESG goals and initiatives into action plans and engagement.

● *REPRESENTATIVE TPRM ESG INITIATIVES*

- Environmental:
  - Review baseline assessment of carbon footprint and/or environment risk and opportunity assessment.
  - Understand management considerations regarding energy use.
  - Evaluate environmental supply chain and consider sources of key third-party data relevant to calculating Level 1, 2, and 3 emissions.
- Social:
  - Request policies on workforce diversity and modern slavery.
  - Review formal programs to promote community service/involvement.
- Governance:
  - Request corporate social responsibility policy.
  - Inquire about corporate entertainment policy/gifting and executive compensation.
  - Request cyber and data privacy policy.
  - Request anti-bribery policy.

Conclusion

The global business community is facing a wider range of risks than ever before, and third-party risk remains a significant and poorly understood vulnerability for most companies. That's exactly why an increasing number of business leaders, audit committees, and board members are asking questions and prioritizing TPRM. The time truly is now to ensure that your organization understands how its third parties connect with and impact critical business processes, and takes action to transfer or mitigate risk where needed.

Third-party risk management doesn't necessarily mean you won't work with third parties that don't meet certain criteria. Instead, **effective TPRM means that — throughout the third-party life cycle — you're doing the due diligence to understand and monitor the risk they present, and building strategic partnerships that enable you to work together to mitigate that risk**. In this way, TPRM also becomes a path to building better, stronger partnerships with your third parties.

Regardless of an organization's size, business model, or budget, TPRM is a continuous journey. Every company is still learning, especially when it comes to emerging and fast-changing risks like ESG, cybersecurity, and personal data privacy. Confusion abounds whether you're the contracting organization or the third party trying to comply with customer requests — but **as we all continue our journey to understanding how best to identify and manage third-party risk, we have an invaluable opportunity to learn from one another.**

Every business can learn a great deal from current TPRM trends, and every business can benefit from taking some key steps forward on the path to TPRM maturity. Start by getting leadership more involved, undertaking a TPRM maturity assessment, and prioritizing TPRM initiatives based on risk. Evaluate your cyber insurance policy or consider if cyber insurance is an appropriate risk management strategy for your business — considering the organization's readiness to align with policy requirements around cybersecurity. Last but not least, work on building out your continuous monitoring capabilities, giving your organization the best chance for effective and timely identification, mitigation, and responses to third-party risks and events. **As your TPRM journey continues, these are key ways you can reduce your third-party risk — and start to drive value to your organization through TPRM.**

About the Authors

Amy Feldman

Director, Security, Privacy and Risk

RSM US LLP

Oliver Snavely

Director, Process Risk and Controls

RSM US LLP

Amy currently serves as a director in RSM's independent security controls practice, focusing on third-party risk management services. With over 10 years of experience consulting in security, privacy, and risk management services across a variety of industries, Amy focuses on helping her clients build, implement, and assess their third-party risk management programs aligning to industry best practices as defined by Shared Assessments, the Third Party Risk Association, and a variety of governance frameworks and compliance requirements.

Prior to following her passion in third-party risk management, Amy oversaw the project management office (PMO) for security and privacy risk consulting where she was responsible for the centralized and coordinated management of all consulting processes and delivery of engagements within the security and privacy risk consulting practice.

Oliver provides risk advisory, process improvement, internal audit, and third-party risk management services. His experience has crossed a number of industries including technology, telecommunications, media, real estate, and life science. Additionally, Oliver has provided audit and consulting services to private equity fund portfolio companies across industries and focuses on key areas that drive value creation such as process optimization and risk mitigation. Oliver is a private equity and third-party risk management leader within the firm's Risk Consulting practice.

Richard Marcus

VP of Information Security
AuditBoard

John Volles

Director of Information Security Compliance
AuditBoard

Richard is the VP of Information Security at AuditBoard, where he leads product, infrastructure, and corporate IT security functions as well as AuditBoard's own internal risk and compliance initiatives. In this capacity, he has become an AuditBoard product power user, leveraging the platform's robust feature set to help achieve SOC 2, GDPR, ISO 27001 certification, and many other GRC initiatives. In his spare time, he enjoys exchanging insights with his information security leader peers in the AuditBoard Community and participating in the AuditBoard product development process. Prior to joining AuditBoard, Richard led global GRC at Verizon Media and Security Operations at EdgeCast Networks.

John is a Director of Information Security Compliance responsible for overseeing AuditBoard's compliance, risk, and privacy obligations as well as helping customers understand AuditBoard's security posture and position. John joined AuditBoard from EY, where he reviewed and implemented client compliance programs and supporting technologies.

About AuditBoard

AuditBoard is the leading cloud-based platform transforming audit, risk, and compliance management. More than 40% of the Fortune 500 leverage AuditBoard to move their businesses forward with greater clarity and agility. AuditBoard is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the fourth year in a row as one of the fastest-growing technology companies in North America by Deloitte. To learn more, visit: AuditBoard.com.

About RSM

RSM US LLP is an audit, tax, and consulting firm focused on the middle market in the United States and Canada and is a member of the global accounting network RSM International. As the leading provider of professional services to the middle market, our vision is to be known globally for delivering innovative solutions, lasting value and confidence. Our global purpose is to instill confidence in a world of change. We do this through our strategy and our culture, which is a powerful competitive advantage that differentiates RSM as the leading provider of assurance, tax and consulting services for middle market companies, the thought leader on the issues clients care about most, and a leader in inclusive and compelling talent experiences.