Deloitte.

Maturing third party risk management with next-gen risk intelligence data and capabilities

A look into the role of emerging external data and capabilities in third party risk management (TPRM)

Introduction

In recent years, third party use has drastically increased as companies realize the value of utilizing third parties to drive efficiencies and foster innovation to enable focus on core competencies. As the third party ecosystem grows, so does the exposure to increasingly sophisticated threat actors capitalizing on technology advancements.

Organizations should transform their approach to third party risk to effectively manage risk at scale, enable quicker decision-making when risks arise or incidents occur, and ultimately adapt to a rapidly changing risk landscape and increasing regulatory expectations.

In this paper, Deloitte explores how your organization can effectively mature toward a more dynamic third party risk management program, shifting focus from static or point-in-time to more proactive risk sensing. We will dive into how you can integrate risk intelligence data and capabilities across all stages of your third party risk management (TPRM) lifecycle to enhance risk management processes to gain insight into emerging third party risks, all while enabling smarter decision-making for your third party risk management program and broader organization.

Table of contents

03 **Keeping pace with the changing third party risk landscape**

Driven by heightened regulatory expectations, a growing threat landscape, and increasing risk of operational disruption, traditional approaches to managing third party risk may no longer be adequate.

06 **Emerging capabilities to meet changing risk management needs**

Risk intelligence data and capabilities drive faster response, increased operational resilience, efficiency gains, and enhanced due diligence while enabling proactive decision-making.

07 **Applying next-gen capabilities across the third party lifecycle**

Risk intelligence can be used to strengthen the effectiveness each step of your organization's third party risk management lifecycle. Merging traditional and emerging third party risk management practices involves aligning people, processes, and technology with your organizational goals.

11 **How Deloitte can help**

Our breadth and depth of services can help your organization design and implement leading practices and processes for continuous monitoring tools and capabilities. Connect with us to learn more.

Keeping pace with the changing third party risk landscape

As sophisticated threats to supply chains emerge, traditional methods for managing third party risk have fallen behind. Recent widely disruptive events over the last few years (e.g., MOVEit, SolarWinds, COVID-19 pandemic and supply chain shortages) are driving heightened attention on operational resilience and cybersecurity among government agencies and regulating bodies, thereby increasing pressure on organizations to enhance third party risk capabilities.

Major drivers for change:

Increasing regulatory scrutiny

- The SEC recently adopted rules[1] on cybersecurity risk management, strategy, governance, and incident disclosure by public companies in the US
- US and Canadian regulating agencies recently published new guidance for financial institutions on managing third party risk[2]

Growing threat landscape

- Threats are becoming increasingly sophisticated, driving greater risk across the third party ecosystem in both costs and customer trust in the event of an incident
- Globally, the average total cost of a data breach in 2022 was USD $4.45M, representing a 15.3% increase since 2020[3]

Advancing technology & innovation

- As threat actors leverage new and innovative technologies like generative artificial intelligence (AI) for malicious attacks, organizations must focus on advancing defensive strategies
- Proactive risk sensing reduces risk by enabling organizations to identify warning signs

Cloud concentration risk

- Many organizations are migrating to cloud services, exposing them to risks associated with hosting information in the cloud
- Organizations will need to diversify the distribution of information hosted in the cloud, both from a third party and a geographical perspective

Increasing risk of disruption

- Greater reliance on an extended third party ecosystem to support critical business processes means greater risk of operational disruption
- Businesses are increasingly focused on identifying operational risks and proactively mitigating to reduce risk of disruption

Need for efficiency gains

- Many organizations struggle with a 'check-the-box'/compliance focused approach to managing third party risk
- Assessment fatigue, frustrated business partners, long time to market, and inefficient use of resources that hinders scalability and true risk management are common

[1] Securities and Exchange Commission (SEC)—Final Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (September 2023)
[2] OSFI: B-10 Third Party Risk Management Guideline (April 2023); Interagency Guidance on Third Party Relationships: Risk Management (June 2023)
[3] Cost of a Data Breach 2023 | Research conducted independently by Ponemon Institute

Maturing our risk-based approach to meet changing risk management needs

Transitioning to a true risk-based approach requires an understanding of the inherent risk exposures and reliance on the service, in addition to a clearly articulated approach for identifying levels of risk to focus assessment on the most important risk exposures.

Balancing "compliance" expectations with true risk management

01 Tier Based Assessment

- High inherent risk and critical third-party arrangements must receive an annual full control assessment
- Medium risk arrangements assessed bi-annually

02 Risk Based Assessment & Monitoring

An operational resilience-driven assessment program focused on major exposures with defined thresholds

e.g., cyber driven operational failures, network connectivity resulting in major loss of PII…

Based on identified inherent risk exposures, certain controls are assessed periodically / continuously

External insights or exposures may support assessment or prompt deeper review / application of additional capabilities

Findings Management & Remediation

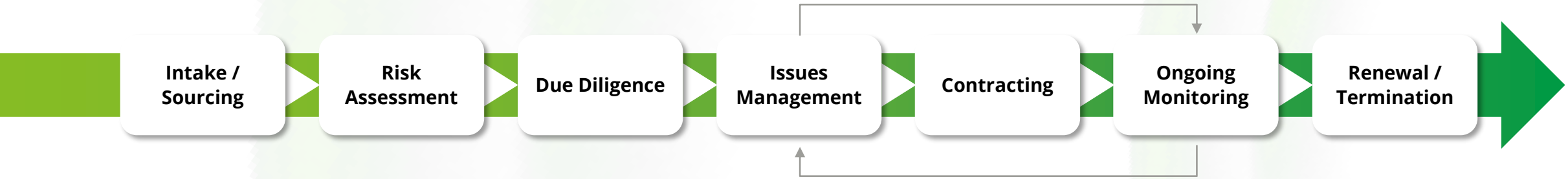
 |

Third party risk needs processes that can move faster

The traditional TPRM program takes a cadence-based, point-in-time approach to evaluating the control posture of third parties, often missing emerging risks. Recent events have proven that there is a need to transition programs from the stand-alone traditional lifecycle toward an integrated operational approach to drive continuous insight into third-party risk exposures.

Traditional end-to-end lifecycle

Evaluates third-party control effectiveness, relative to the service being delivered, on a cadence dictated by risk tier



&

Operational monitoring lifecycle

Continuously evaluates third-party control effectiveness and emerging risks using both internal and external data

 |

Emerging and next-gen third party risk capabilities

Leveraging next-gen risk intelligence data and capabilities enables organizations to transfer much of the cost and effort of today's traditional processes to an integrated, holistic, and more proactive approach that combines internal and external data and capabilities for higher value risk management and faster identification of emerging risks.

What next-gen capabilities are emerging in TPRM?

There are several innovative capabilities emerging that can be used to monitor or sense risk across various in-scope domains to better understand the risk across a third party and supply chain risk landscape. Emerging tools and capabilities can be used to identify potential risk exposures, vulnerabilities, threats and events, aggregate data and understand trends, and enable better decision-making across your organization

Dimensions of next-gen capabilities...

- AI-enabled TPRM practice automation
- Aggregate risk dashboarding
- Detection of extended ecosystem, risk exposures & concentrations
- Cyber hygiene scoring and trending of internet facing assets
- Illumination of technology and applications used by third parties
- AI-enabled risk sensing and alerting for abnormal activity

Growth of data availability across domains...

External data sources continue to become more available and mature across a variety of domains.

- ABAC/Sanctions
- AI
- Cloud
- Compliance
- Concentration
- Country
- Cyber
- ESG
- Financial Viability
- Fraud/AML
- Health & Safety
- Physical Security
- Privacy
- Resilience
- Subcontractor

As data matures, organizations should consider the level of data needed based on desired outcomes such as gaining aggregate insights, increasing efficiency, or enabling operational alerting.

Maturing data sources

Organizations vary in next-gen risk sensing/monitoring maturity

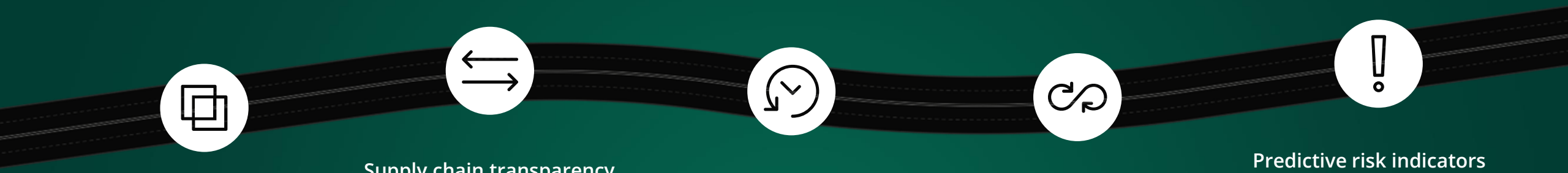
Many organizations are licensing cyber monitoring data and capabilities to complement/enhance risk assessments and drive proactive risk management

Some organizations are building risk sensing and workflow/alerting capabilities on top of risk aggregation technology to enable broad risk operational monitoring

More mature organizations are beginning to stand up dedicated security operation center-like capabilities for third party threat intelligence and incident response

Applying next-gen capabilities across the third party lifecycle

Emerging capabilities and data can be applied across every step of the third party management lifecycle to enhance efficiency of current processes, build scalability, and drive proactive management of third party risk. Use cases vary in return on investment and benefit based on your organizational goals.



Pre-contract

Third Party Prescreen

Quickly pre-screen third party candidates for viability across priority risk domains in alignment with your organizational strategy

Reduce Time to Market:

Streamline upfront due diligence processes through agile, rules-based assessment scoping and response validation and challenge

Supply chain transparency

Identify Concentrations

Use fourth party and fifth party detection to identify geographic and dependence risks from both an industry and organizational perspective

Identify Ecosystem Risks

Uncover risk exposures in your extended service provider ecosystem resulting from service disruptions

Assessment efficiency

Focused Assessment Scoping and Deferral Opportunities

Apply data to control assessments to enable rules-based scoping and focus resources on real risk exposures; Enable deferrals by leveraging data to determine whether deeper assessment is warranted

Corroborate and Challenge

Confirm or challenge control assessment responses using data

Ongoing monitoring

Increase Breadth of Coverage

Apply monitoring to broader segments of your portfolio

Increase Depth of Coverage

Gain deeper risk insights through capabilities like technical network enumeration and data flow analysis to uncover cyber risks

Accelerated Response

Perform faster impact analysis and incident response when risks or events are identified

Predictive risk indicators

Proactive Risk Sensing and Threat Intelligence

Use monitoring data, threat intelligence and correlation/analytics to sense risk indicators and apply proactive control measures

Third Party Advisories

Use data sources to develop internal third party threat advisories to equip internal teams with insight into the risk and threat landscape to proactively drive down risk

AI capabilities driving efficiency & automation

- Machine learning (ML) can be used to develop prescreen rulesets for risk domain prioritization based on business context and analyze public records for fourth- and fifth-party relationship mapping and risk identification
- Natural language processing (NLP) can be used to ingest and validate third party control assessments and standardized reports (e.g., SOC reports)

Use cases in action:

- Proactive risk sensing and threat intelligence
- Accelerated response

Applying proactive risk sensing & threat intelligence to take action prior to an incident

A look at how using next-gen capabilities can help your organization take a proactive approach to third party cyber risk by sensing drops in cyber hygiene and identifying vulnerabilities likely to be exploited.

The scenario: Third party data breach

Your organization was notified by a third party that it recently suffered a severe data breach through an exploited software vulnerability, affecting a large volume of personally identifiable customer data. This incident could result in financial, operational, reputational, and even regulatory impacts for both your organization and the third party, depending on the nature of the breach.

Without next-gen capabilities, organizations are likely to handle such an event in a reactive manner – relying on cadence-based control assessments to identify control gaps or depending on the third party to disclose the breach, then triggering incident response protocols and filing a cyber insurance claim. Response to the event is likely inefficient as organizations seeks to identify which other third parties may be at risk or impacted by the breach.

With next-gen capabilities, you could....

- Leverage external vulnerability data and threat intelligence to identify high severity third party vulnerabilities that are being actively exploited in the wild by malicious threat actors, allowing your resources to stay ahead by promptly prioritizing action with the third party before an event occurs.
- Apply monitoring rulesets to sense significant changes in cyber hygiene in relevant areas (such as credential management, application security, or patch management) based on your use of the third party. This method can be used to sense risks proactively, enabling you to take measures to manage your exposure.
- Leverage technology stack illumination and vulnerability monitoring capabilities to gain transparency into software products being used by your third parties to identify risks in your extended ecosystem.
- When an incident occurs in your broader supply chain, apply extended ecosystem detection and tech stack illumination capabilities to evaluate the breadth of impact across your third party portfolio and accelerate your response.

Use cases in action:

- Identify ecosystem risks

Applying supply chain transparency to identify ecosystem risks and disruptions

A look at how using next-gen capabilities can help your organization identify potential exposures across the extended third party ecosystem that may cause operational disruption to you through your direct third parties.

The scenario: Fourth party business disruption

A card plastics provider to your direct third party experiences a labor strike that results in a temporary shut-down of services to your direct third party. Due to your third party's relationship with the fourth party, this event will likely affect your organization's ability to provide new cards to your customers in a timely manner, resulting in customer impacts and potential loss of business.

Without next-gen capabilities, organizations may only become aware of this event when the direct third party notifies of a disruption, which may result in a delayed response and initiation of your contingency plan.

With next-gen capabilities, you could....

- Automatically detect fourth party (and beyond) relationships within your third party ecosystem to understand and gain transparency into your extended supply chain risks that can affect your organization, including identification of fourth party concentrations.
- Apply monitoring rulesets to prioritized fourth party relationships such as those that are concentrated, supporting critical third party services, or processing sensitive data to sense emerging risks. Cross-domain *(e.g., cyber, ESG, regulatory)* risk sensing may be applied based on the type of service provided to enable proactive identification and response.
- Post-event, use next-gen capabilities to evaluate the breadth of impact across your third party portfolio by understanding which direct third parties may be affected by the event, and further, where your organization may experience operational disruptions (triggering contingency plans) or data loss.

Harnessing next-gen capabilities to enhance third party risk management

Realizing the full potential of next-gen risk intelligence data and capabilities requires consideration across people, processes, data, and technology, enabling your TPRM program to align with strategic enterprise objectives, increased regulatory scrutiny, and keep pace with changing risk landscape. The most effective programs take a balanced approach between traditional practices and next-gen capabilities.

People

Resources with integrated skillset

Upskill talent to include both third party and cyber risk domain expertise that can integrate cross-domain risk knowledge; build skillsets for development of program strategy, traditional assessment, and day-to-day operational monitoring, response and remediation.

Process

Risk prioritization methodology

Define standard practices to gain relevant, proactive, and prioritized insights…

- Prioritization methodology, correlation rules & alert thresholds
- Fourth party scope & criteria
- Analysis & response playbooks

Technology

Unified technology and architecture

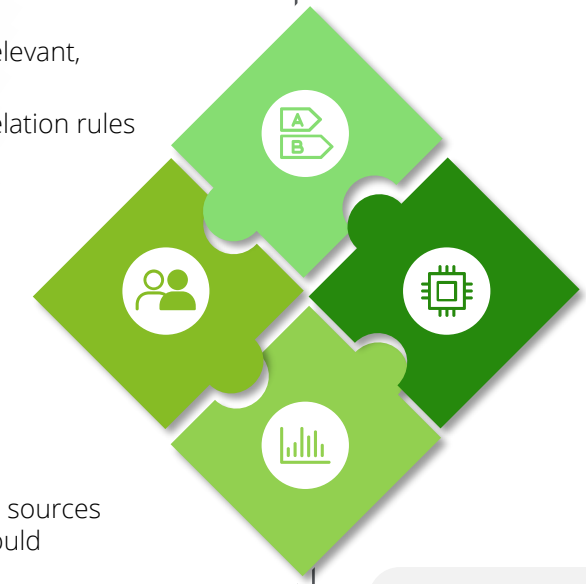
Articulate technology and data architecture / strategy to meet the program's objectives and enable enhanced practices, including…

- Internal/external data ingestion
- Central data lake and AI-enabled correlation
- Alerting, workflow and ticketing
- Dashboard and reporting capabilities

Data

Accurate data sources

Leverage internal and external data sources to gain actionable insights. Data should include internal data (from TPRM, Procurement, etc.) to determine relevance and potential impact of external risks and events, threat intelligence & vulnerability data, cross-risk and historical data on prior incidents, and fourth/fifth party relationship and technology detection.



Align with heightened regulatory expectations using next-gen capabilities to drive…

- Faster impact analysis and determination of material third party cyber incidents
- Ability to demonstrate cybersecurity risk management strategy including identification, assessment, and management of third party cyber risks
- Enhanced governance and reporting of third party cyber risks

Risk intelligence data and capabilities can help your organization to more effectively identify, assess, and determine materiality of third party incidents faster – reducing your exposure and helping you to demonstrate alignment with regulatory expectations

How Deloitte can help

Understanding that organizations are at different points in their TPRM journey, we have outlined ways you can leverage Deloitte's innovative approaches to integrate next-gen risk intelligence data and capabilities into your program. Our advisory services can help your organization design and implement leading practices and processes, while our managed services can expedite operationalization.

We can help your organization at every step of the way…

- Perform a benchmark analysis of your current program readiness for next-gen capabilities using our maturity model
- Develop a strategic roadmap to introduce next-gen capabilities into your program for risk management enhancement and efficiency gains
- Build or enhance your data and technology strategy (e.g. reference architecture and technology stack) to integrate data sources for improved insight
- Integrate priority use cases & develop supporting playbook/ process documentation for consistent execution using next-gen capabilities
- Perform resource gap analysis and define requirements to build an operating model that can support enhanced capabilities
- Support development and integration of AI models within your program for efficiency gains and enhanced risk sensing across functions

Managed services

Fully outsource or augment your program with Deloitte's managed services to:

- Leverage experienced professionals and innovative technology performing activities on your behalf
- Expedite the operationalization of your desired capabilities in support of your broader strategic goals

Advise & implement services

Accelerate and scale your third party risk management program capabilities through collaboration with Deloitte, tapping into our extensive experience and capabilities. We can support you on your next-gen TPRM journey as you consider…

- Selecting and implementing new external risk intelligence data or capabilities
- Enhancing your program to gain greater efficiency and risk management outcomes
- Introducing advanced threat intelligence and risk response capabilities as an extension of your Security Operations Center

We can help you get to where you want to be.

Connect with us

Discuss the report and learn more about our approach.

Suzanne Denton
Managing Director
Deloitte & Touche LLP
sudenton@deloitte.com

Michael Nassar
Partner
Deloitte LLP
minassar@deloitte.ca

Jon Rizzo
Principal
Deloitte & Touche LLP
jonrizzo@deloitte.com

Karan Singh
Managing Director
Deloitte & Touche LLP
karansignh@deloitte.com

Walt Hoogmoed
Partner
Deloitte & Touche LLP
whoogmoed@deloitte.com

Contributors

Chetan Bhogal
Consultant
Deloitte LLP

Nicole Johnson
Manager
Deloitte & Touche LLP

Jared Wood
Senior Consultant
Deloitte & Touche LLP

Talea Zuk
Manager
Deloitte LLP

Deloitte.

Thank you.